13 User Access and Authentication Commands

13.1 AAA Configuration Commands

13.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.1.2 aaa

Function

The **aaa** command displays the AAA view.

Format

aaa

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Using the **aaa** command in the system view, you can enter the AAA view and perform the following security configurations for access users:

- Creating users
- Configuring user levels
- Creating an authentication scheme
- Creating an authorization scheme
- Creating a domain

Example

Access the AAA view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa]
```

13.1.3 aaa abnormal-offline-record

Function

The **aaa abnormal-offline-record** command enables the device to record users' abnormal logout information.

The **undo aaa abnormal-offline-record** command disables the device from recording users' abnormal logout information.

By default, the device records users' abnormal logout information.

Format

aaa abnormal-offline-record

undo aaa abnormal-offline-record

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If users abnormally log out, run **aaa abnormal-offline-record** command to enable the record function for fault locating.

After the **undo aaa abnormal-offline-record** command is run, no abnormal logout information is recorded unless the **aaa abnormal-offline-record** command is run.

Example

Enable the device to record users' abnormal logout information.

```
<HUAWEI> system-view
[HUAWEI] aaa abnormal-offline-record
```

Disable the device from recording users' abnormal logout information.

```
<HUAWEI> system-view
[HUAWEI] undo aaa abnormal-offline-record
```

13.1.4 aaa offline-record

Function

The **aaa offline-record** command enables the device to record users' normal logout information.

The **undo aaa offline-record** command disables the device from recording users' normal logout information.

By default, the device is enabled to record user normal logout information.

Format

aaa offline-record

undo aaa offline-record

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If users fail to get online, run **aaa offline-record** command to enable the record function for fault locating.

After the **undo aaa offline-record** command is run, no logout information is recorded unless the **aaa offline-record** command is run.

Example

Enable the device to record users' normal logout information.

```
<HUAWEI> system-view
[HUAWEI] aaa offline-record
```

Disable the device from recording users' normal logout information.

```
<HUAWEI> system-view
[HUAWEI] undo aaa offline-record
```

13.1.5 aaa online-fail-record

Function

The **aaa online-fail-record** command enables the device to record users' online failures.

The **undo aaa online-fail-record** command disables the device from recording users' online failures.

By default, the device records users' online failures.

Format

aaa online-fail-record

undo aaa online-fail-record

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If you want to query the login failure records to find out unauthorized users, run the **aaa online-fail-record** command to enable the device to record users' online failures.

After the **undo aaa online-fail-record** command is run, no online failure is recorded unless the **aaa online-fail-record** command is run.

Example

Enable the device to record users' online failures.

```
<HUAWEI> system-view
[HUAWEI] aaa online-fail-record
```

Disable the device from recording users' online failures.

```
<HUAWEI> system-view
[HUAWEI] undo aaa online-fail-record
```

13.1.6 aaa-authen-bypass

Function

The **aaa-authen-bypass** command sets the bypass authentication timeout interval.

The **undo aaa-authen-bypass** command cancels the bypass authentication timeout interval.

By default, no bypass authentication timeout interval is set.

Format

aaa-authen-bypass enable time *time-value*

undo aaa-authen-bypass enable

Parameters

Parameter	Description	Value
enable	Enables remote bypass authentication.	-
time *time-value*	Specifies the bypass authentication timeout interval.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the scenarios that require fast authentication response. When a user in a user domain where multiple authentication modes (for example, RADIUS authentication and local authentication) are configured, bypass authentication is enabled, and the bypass authentication timeout interval is configured, the user will be authenticated using the local authentication mode and the bypass authentication timer is enabled simultaneously if the RADIUS server does not respond to the authentication request. When other users in the same domain are authenticated during the configured bypass authentication timeout interval, the users are directly authenticated using the local authentication mode, so that the users can be authenticated without waiting until the RADIUS server responds to their authentication requests, accelerating the authentication response.

Precautions

When only one authentication mode is configured in a user domain and the bypass authentication timer is enabled, other users in the same domain are directly considered to fail the authentication during the bypass authentication timeout interval.

Example

Set the bypass authentication timeout interval to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa-authen-bypass enable time 3
```

13.1.7 aaa-author-bypass

Function

The **aaa-author-bypass** command sets the bypass authorization timeout interval.

The **undo aaa-author-bypass** command cancels the bypass authorization timeout interval.

By default, no bypass authorization timeout interval is set.

Format

aaa-author-bypass enable time *time-value*

undo aaa-author-bypass enable

Parameters

Parameter	Description	Value
enable	Enables remote bypass authorization.	-
time *time-value*	Specifies the bypass authorization timeout interval.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the scenarios that require fast authorization response. When a user in a user domain where multiple authorization modes (for example, HWTACACS authorization and local authorization) are configured, bypass authorization is enabled, and the bypass authorization timeout interval is configured, the user will be authorized using the local authorization mode and the bypass authorization timer is enabled simultaneously if the HWTACACS server does not respond to the authorization request. When other users in the same domain are authorized during the configured bypass authorization timeout interval, the users are directly authorized using the local authorization mode, so that the users can be authorized without waiting until the HWTACACS server responds to their authorization requests, accelerating the authorization response.

Precautions

When only one authorization mode is configured in a user domain and the bypass authorization timer is enabled, other users in the same domain are directly considered to fail the authorization during the bypass authorization timeout interval.

Example

Set the bypass authorization timeout interval to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa-author-bypass enable time 3
```


13.1.8 aaa-author-cmd-bypass

Function

The **aaa-author-cmd-bypass** command sets the command-line bypass authorization timeout interval.

The **undo aaa-author-cmd-bypass** command cancels the command-line bypass authorization timeout interval.

By default, no command-line bypass authorization timeout interval is set.

Format

aaa-author-cmd-bypass enable time *time-value*

undo aaa-author-cmd-bypass enable

Parameters

Parameter	Description	Value
enable	Enables remote command-line bypass authorization.	-
time *time-value*	Specifies the command-line bypass authorization timeout interval.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the scenarios that require fast command-line authorization response. When a user in a user domain where multiple command-line authorization modes (for example, HWTACACS authorization and local authorization) are configured, command-line bypass authorization is enabled, and the command-line bypass authorization timeout interval is configured, the user will be authorized using the local authorization mode and the command-line bypass authorization timer is enabled simultaneously if the HWTACACS server does not respond to the command-line authorization request. When other users in the same domain are authorized during the configured command-line bypass authorization timeout interval, the users are directly authorized using the local authorization mode, so that the users can be authorized without waiting until the

HWTACACS server responds to their authorization requests, accelerating the authorization response.

Precautions

When only one command-line authorization mode is configured in a user domain and the command-line bypass authorization timer is enabled, other users in the same domain are directly considered to fail the command-line authorization during the command-line bypass authorization timeout interval.

Example

Set the command-line bypass authorization timeout interval to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa-author-cmd-bypass enable time 3
```

13.1.9 aaa-author session-timeout invalid-value enable

Function

The **aaa-author session-timeout invalid-value enable** command prevents a device from disconnecting or reauthenticating users when the RADIUS server delivers session-timeout with value 0.

The **undo aaa-author session-timeout invalid-value enable** command restores the default setting.

By default, when the RADIUS server delivers session-timeout with value 0, this attribute does not take effect.

Format

aaa-author session-timeout invalid-value enable

undo aaa-author session-timeout invalid-value enable

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

When the RADIUS server delivers session-timeout with value 0:

- If the **aaa-author session-timeout invalid-value enable** command is not configured, the session-timeout attribute delivered by the server does not

take effect and the period for disconnecting or reauthenticating users depends on the device configuration.

- If the **aaa-author session-timeout invalid-value enable** command is configured, the session-timeout attribute delivered by the server takes effect and the device does not disconnect or reauthenticate users.

You can run the **dot1x timer reauthenticate-period** *reauthenticate-period-value* or **mac-authen timer reauthenticate-period** *reauthenticate-period-value* command to configure the period for disconnecting or reauthenticating users on the device.

Example

Prevent the device from disconnecting or reauthenticating users when the RADIUS server delivers session-timeout with value 0.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] aaa-author session-timeout invalid-value enable
```

13.1.10 aaa-quiet administrator except-list

Function

The **aaa-quiet administrator except-list** command configures a user to access the network using a specified IP address when the user account is locked.

The **undo aaa-quiet administrator except-list** command restores the default setting.

By default, a user cannot access the network when the account is locked.

Format

aaa-quiet administrator except-list { *ipv4-address* | *ipv6-address* } &<1-32>

undo aaa-quiet administrator except-list

Parameters

Parameter	Description	Value
ipv4-address	Specifies an IPv4 address. A user can access the network using this IPv4 address when the user account is locked.	The value must be a valid unicast address in dotted decimal notation.

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address. A user can access the network using this IPv6 address when the user account is locked.	The total length of the value is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format of X:X:X:X:X:X:X:X.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In AAA view, after the function of locking the account of an AAA local authentication user or AAA remote authentication user is configured using the **local-aaa-user wrong-password** or **administrator remote authen-fail** command, if a user consecutively enters an incorrect password and the number of times that the user enters an incorrect password reaches the allowed maximum number of times, the user account is locked and the user cannot access the network when the account is locked. To facilitate maintenance and management, you can run the **aaa-quiet administrator except-list** command to configure the user to access the network using a specified IP address when the user account is locked.

Precautions

- This function takes effect only for the administrators.
- A maximum of 64 IPv4 and IPv6 addresses can be configured.

Example

Configure a user to access the network using the specified IP address 10.1.1.1 when the user account is locked.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] aaa-quiet administrator except-list 10.1.1.1
```


13.1.11 access-limit user-name max-num

Function

The **access-limit user-name max-num** command configures the maximum number of users who are allowed to access the network using the same user name.

The **undo access-limit user-name max-num** command restores the default setting.

By default, the number of users who are allowed to access the network using the same user name is not limited, and is determined by the maximum number of access users supported by the device.

Format

access-limit user-name max-num *number*

undo access-limit user-name max-num

Parameters

Parameter	Description	Value
number	Specifies the maximum number of users who are allowed to access the network using the same user name.	The value is an integer and is determined by the maximum number of access users supported by the device.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

By default, the number of users who are allowed to access the network using the same user name is not limited. To limit the number of users who are allowed to access the network using a user name, run the **access-limit user-name max-num** command. For example, the bandwidth share mode is configured for all terminal users in a small office network access scenario. To facilitate maintenance, the server delivers the same user name to replace the user names entered by terminal users. The number of access users needs to be limited based on the user name to ensure the network access experience of all terminal users.

For RADIUS authentication users, configurations for limiting the number of access users based on the user name are carried in the HW-UserName-Access-Limit (26-18) attribute.

NOTE

Only users who are successfully authenticated support the configurations for limiting the number of access users based on the same user name, and pre-connection users do not support such configurations.

This command does not take effect in inter-AC roaming scenarios.

Example

In the service scheme **s1**, set the maximum number of users who are allowed to access the network using the same user name to 15.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] access-limit user-name max-num 15
```

13.1.12 accounting dual-stack separate

Function

The **accounting dual-stack separate** command enables separate statistics collection or separate rate limiting of IPv4 and IPv6 user traffic.

The **undo accounting dual-stack separate** command disables separate statistics collection or separate rate limiting of IPv4 and IPv6 user traffic.

By default, the device does not distinguish between IPv4 and IPv6 user traffic when collecting traffic statistics or rate limiting IPv4 and IPv6 user traffic.

NOTE

This command is supported only on the following switch models:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI

Format

accounting dual-stack separate

undo accounting dual-stack separate

Parameters

None

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect statistics about IPv4 and IPv6 user traffic separately or perform accounting for IPv4 and IPv6 users separately based on traffic, run the **statistic enable (AAA domain view)** command to enable traffic statistics collection, and then run the **accounting dual-stack separate** command to enable separate traffic statistics collection for IPv4 and IPv6 users.

If you want to separately limit the rate of IPv4 and IPv6 users based on traffic, authorize CAR to the users, and then run the **accounting dual-stack separate** command to enable separate rate limiting for IPv4 and IPv6 users.

Precautions

You are advised to configure this function before users go online. If this function is configured after users go online, separate traffic statistic collection or rate limiting may be inaccurate. You are advised to collect traffic statistics or limit the rate again after users go offline.

Example

Enable separate statistics collection or separate rate limiting of IPv4 and IPv6 user traffic.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain example
[HUAWEI-aaa-domain-example] accounting dual-stack separate
Warning: This operation may cause online users' traffic statistics inaccurate, Re-online is recommended after this operation, continue?[Y/N]y
```

13.1.13 accounting interim-fail

Function

The **accounting interim-fail** command sets the maximum number of real-time accounting failures and configures a policy used after the number of real-time accounting failures exceeds the maximum.

The **undo accounting interim-fail** command restores the default maximum number of real-time accounting failures and the default policy.

By default, the maximum number of real-time accounting failures is 3 and the device keeps users online after the number of real-time accounting failures exceeds the maximum.

Format

accounting interim-fail [**max-times** *times*] { **offline** | **online** }

undo accounting interim-fail

Parameters

Parameter	Description	Value
max-times *times*	Specifies the maximum number of real-time accounting failures. If the maximum number of real-time accounting failures is reached and the next accounting request still has no response, the device considers that accounting fails and takes a policy for users.	The value is an integer that ranges from 1 to 255. The default value is 3.
offline	Disconnects users if real-time accounting fails.	-
online	Keeps users online if real-time accounting fails.	-

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the real-time accounting function takes effect, the device sends real-time accounting requests to an accounting server, and the accounting server responds to the accounting requests. If the network is unstable, for example, a jitter occurs, the device may not receive response packets. As a result, accounting is interrupted for a short period of time. To reduce or prevent accounting interruption, run the **accounting interim-fail** command to set the maximum number of real-time accounting failures. The device considers that real-time accounting fails only after the number of consecutive real-time accounting failures exceeds the maximum.

Choose one of the following policies to be applied after the maximum number of real-time accounting failures is reached:

- **online**: To prevent users from being affected by network faults, use the **online** policy to allow paid users to go online.
- **offline**: To stop providing services when accounting fails, use the **offline** policy to force paid users to go offline.

Prerequisites

The real-time accounting function has been enabled by using the **accounting realtime** command.

Precautions

The **accounting interim-fail** command does not take effect for online users, but takes effect for the users who go online after the command is executed.

Example

In the accounting scheme **scheme1**, set the maximum number of real-time accounting failures to 5 and use the **offline** policy.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1] accounting realtime 3
[HUAWEI-aaa-accounting-scheme1] accounting interim-fail max-times 5 offline
```

13.1.14 accounting realtime

Function

The **accounting realtime** command enables the real-time accounting function and sets the interval for real-time accounting in an accounting scheme.

The **undo accounting realtime** command disables the real-time accounting function.

By default, the device performs accounting based on user online duration, the real-time accounting function is disabled.

Format

accounting realtime *interval*

undo accounting realtime

Parameters

Parameter	Description	Value
interval	Specifies the interval for real-time accounting.	The value is an integer that ranges from 0 to 65535, in minutes. When the value is set to 0, real-time accounting is disabled. The default value is 0.

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the users who are charged based on online duration. If a user goes offline unexpectedly, the accounting server cannot receive the accounting-stop packet, so it keeps charging the user while they are not receiving a service. To solve the problem, configure the real-time accounting function on the device. After the real-time accounting function is configured, the device periodically sends real-time accounting packets to the accounting server. After receiving the real-time accounting packets, the accounting server charges the user. If the device detects that the user goes offline, it stops sending real-time accounting packets and the accounting server stops accounting. The result of real-time accounting is precise.

Precautions

- When the accounting interval is set using both the **accounting realtime** command and the Acct-Interim-Interval attribute, if the Acct-Interim-Interval value range is 60-3932100, the interval set by Acct-Interim-Interval has a higher priority. Otherwise, the interval set by the **accounting realtime** command takes effect.
- If an accounting scheme is applied to a domain, the **accounting realtime** command does not affect online users, but only takes effect for the users who go online after the command is executed.
- If *interval* is set to 0 and the IP address of the client is changed, the device still sends a real-time accounting packet carrying the changed IP address information to the RADIUS server.
- A short interval for real-time accounting requires high performance of the device and accounting server. If there are more than 1000 users, setting a long interval for real-time accounting is recommended. The following table lists the suggested real-time accounting intervals for different user quantities.

Table 13-1 Real-time accounting interval for different user quantities

User Quantity	Interval for Real-Time Accounting (Minutes)
1-99	3
100-499	6
500-999	12
≥ 1000	≥ 15

Example

In the accounting scheme **scheme1**, enable the real-time accounting function and set the interval for real-time accounting to 6 minutes.


```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1] accounting realtime 6
```

13.1.15 accounting start-fail

Function

The **accounting start-fail** command configures a policy for accounting-start failures.

The **undo accounting start-fail** command restores the default policy for accounting-start failures.

By default, users cannot go online if accounting-start fails. That is, the **offline** policy is used.

Format

accounting start-fail { **offline** | **online** }

undo accounting start-fail

Parameters

Parameter	Description	Value
offline	Rejects users' online requests if accounting-start fails.	-
online	Allows users to go online if accounting-start fails.	-

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user goes online after an accounting scheme is applied, the device sends an accounting-start packet to an accounting server. When the network is working properly, the accounting server responds to the accounting-start packet. If a fault occurs on the network, the device may not receive the response packet from the accounting server. As a result, accounting fails. The device provides the following policies for accounting failures:

- **online**: To prevent users from being affected by network faults, use the **online** policy to allow paid users to go online.
- **offline**: To stop providing services when accounting fails, use the **offline** policy to force paid users to go offline.

Precautions

The command takes effect only when the accounting mode configured using the **accounting-mode** command is HWTACACS or RADIUS.

Example

In the accounting scheme **scheme1**, use the **online** policy for accounting-start failures.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1] accounting start-fail online
```

13.1.16 accounting-mode

Function

The **accounting-mode** command configures an accounting mode in an accounting scheme.

The **undo accounting-mode** command restores the default accounting mode in an accounting scheme.

By default, the accounting mode is **none**.

Format

accounting-mode { **hwtacacs** | **none** | **radius** | **haca** }

undo accounting-mode

Parameters

Parameter	Description	Value
hwtacacs	Indicates that accounting is performed by an HWTACACS server.	-
none	Indicates non-accounting.	-
radius	Indicates that accounting is performed by a RADIUS server.	-

Parameter	Description	Value
haca	Indicates that accounting is performed by an HACA server. **NOTE** Only the following switch models support HACA: S200, S1730S-S1 S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H and S6720S-S	-

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Enterprises or carriers need to generate revenue by charging users who are accessing the Internet.

When a user goes online, accounting starts after the user is authenticated and authorized. When the user goes offline, accounting stops. The client sends the account packet containing the user's online duration to the accounting server.

To charge users, set the accounting mode to RADIUS or HWTACACS. Generally, the accounting mode is consistent with the authentication mode. If you do not need to charge users, set the accounting mode to none.

Precautions

The device does not support local accounting. When the authentication scheme configured using the **authentication-mode** command defines local authentication, you need to run the **accounting-mode none** command to configure non-accounting or run the **accounting start-fail** command to configure a policy for accounting-start failures.

Follow-up Procedure

Apply the accounting scheme to a domain to enable the device to charge the users in the domain using the **domain** command in the AAA view.

Example

Set the accounting mode to RADIUS in the accounting scheme **scheme1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1] accounting-mode radius
```

13.1.17 accounting-scheme (AAA domain view)

Function

The **accounting-scheme** command applies an accounting scheme to a domain.

The **undo accounting-scheme** command restores the default accounting scheme of a domain.

By default, the accounting scheme named **default** is applied to a domain. In this default accounting scheme, non-accounting is used and the real-time accounting function is disabled.

Format

accounting-scheme *accounting-scheme-name*

undo accounting-scheme

Parameters

Parameter	Description	Value
accounting-scheme-name	Specifies the name of an accounting scheme.	The accounting scheme must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To charge users in a domain, create an accounting scheme and perform configurations in the accounting scheme, for example, set the accounting mode and policy for accounting-start failures. Run the **accounting-scheme** command in the AAA domain view to apply the accounting scheme to the domain.

Prerequisites

An accounting scheme has been created and configured using the **accounting-scheme** command. For example, the accounting mode and policy for accounting-start failures have been configured.

Example

Apply the accounting scheme **account1** to the domain **isp1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme account1
[HUAWEI-aaa-accounting-account1] quit
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] accounting-scheme account1
```

Restore the default accounting scheme of the domain **isp2**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain isp2
[HUAWEI-aaa-domain-isp2] undo accounting-scheme
```

13.1.18 accounting-scheme (AAA view)

Function

The **accounting-scheme** command creates an accounting scheme and displays the accounting scheme view.

The **undo accounting-scheme** command deletes an accounting scheme.

By default, there is an accounting scheme named **default** in the system. This default accounting scheme can be modified but cannot be deleted. In this default accounting scheme, non-accounting is used and the real-time accounting function is disabled.

Format

accounting-scheme *accounting-scheme-name*

undo accounting-scheme *accounting-scheme-name*

Parameters

Parameter	Description	Value
accounting-scheme-name	Specifies the name of an accounting scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To charge users in a domain, create and configure an accounting scheme, for example, the accounting mode and policy for accounting-start failures. Run the **accounting-scheme** command in the AAA domain view to apply the accounting scheme to the domain.

Follow-up Procedure

After an accounting scheme is created:

- Run the **accounting interim-fail** command to set the maximum number of real-time accounting failures and configure a policy used after a real-time accounting failure.
- Run the **accounting realtime** command to enable the real-time accounting function and set the interval for real-time accounting in an accounting scheme.
- Run the **accounting start-fail** command to configure a policy for accounting-start failures.
- Run the **accounting-mode** command to configure an accounting mode in an accounting scheme.

After an accounting scheme is configured, run the **accounting-scheme** command in the AAA domain view to apply the accounting scheme to a domain.

Precautions

If the configured accounting scheme does not exist, the **accounting-scheme** command in the AAA view creates an accounting scheme and displays the accounting scheme view. If the configured accounting scheme already exists, the **accounting-scheme** command in the AAA view displays the accounting scheme view directly.

To delete an accounting scheme applied to a domain, run the **undo accounting-scheme (AAA domain view)** command.

Example

Create an accounting scheme named **scheme1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1]
```

Enter the default accounting scheme view.

```
<HUAWEI> system-view
[HUAWEI] aaa
```



```
[HUAWEI-aaa] accounting-scheme default
[HUAWEI-aaa-accounting-default]
```

13.1.19 access-user remote authen-fail

Function

The **access-user remote authen-fail** command enables the account locking function for access users who fail remote authentication.

The **undo access-user remote authen-fail** command disables the account locking function for access users who fail remote authentication.

By default, the account locking function is disabled for access users who fail remote authentication.

Format

access-user remote authen-fail retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

undo access-user remote authen-fail

Parameters

Parameter	Description	Value
retry-interval *retry-interval*	Specifies the authentication retry interval after a remote authentication failure.	The value is an integer in the range from 5 to 65535, in minutes.
retry-time *retry-time*	Specifies the maximum number of consecutive authentication failures.	The value is an integer in the range from 3 to 65535.
block-time *block-time*	Specifies the account locking period.	The value is an integer in the range from 5 to 65535, in minutes.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure account and password security, enable the account locking function for access users who fail remote authentication. If a user reaches the incorrect account or password attempt limit within the specified authentication retry period, the user is locked and will be automatically unlocked after a certain period.

Precautions

- This command takes effect only for remotely authenticated access users.
- When an active/standby switchover is performed, the originally locked account is automatically unlocked.
- After you run the **undo access-user remote authen-fail** command to disable the account locking function for access users who fail remote authentication, the locked account is automatically unlocked.
- If a remote authentication user does not reach the consecutive authentication attempt limit configured using the **access-user remote authen-fail** command, the user is not locked. If you run the **access-user remote authen-fail** command to change the consecutive authentication attempt limit to be less than the number of consecutive authentication failures, the user has one chance to be authenticated.

Example

Enable the account locking function for access users who fail remote authentication, and set the authentication retry interval to 5 minutes, maximum number of consecutive authentication failures to 3, and account locking period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] access-user remote authen-fail retry-interval 5 retry-time 3 block-time 5
```

13.1.20 administrator remote authen-fail

Function

The **administrator remote authen-fail** command enables the account locking function for administrators who fail remote authentication.

The **undo administrator remote authen-fail** command disables the account locking function for administrators who fail remote authentication.

By default, the account locking function is enabled for administrators who fail remote authentication, the authentication retry interval is 5 minutes, the maximum number of consecutive authentication failures is 30, and the account locking period is 5 minutes.

Format

administrator remote authen-fail retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

undo administrator remote authen-fail

Parameters

Parameter	Description	Value
retry-interval *retry-interval*	Specifies the authentication retry interval after a remote authentication failure.	The value is an integer in the range from 5 to 65535, in minutes.
retry-time *retry-time*	Specifies the maximum number of consecutive authentication failures.	The value is an integer in the range from 3 to 65535.
block-time *block-time*	Specifies the account locking period.	The value is an integer in the range from 5 to 65535, in minutes.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure account and password security of administrators, enable the account locking function for administrators who fail remote authentication. If an administrator enters incorrect account and password more than the maximum number of consecutive authentication failures within the given period, the account is locked. After a certain period, the account is unlocked.

Precautions

- This command takes effect only for remotely authenticated administrators.
- When an active/standby switchover is performed, the originally locked account is automatically unlocked.
- After you run the **undo administrator remote authen-fail** command to disable the account locking function for administrators that fail remote authentication, the locked account is automatically unlocked.
- If a remote authentication user does not reach the consecutive authentication attempt limit configured using the **administrator remote authen-fail** command, the user is not locked. If you run the **administrator remote authen-fail** command to change the consecutive authentication attempt limit to be less than the number of consecutive authentication failures, the user has one chance to be authenticated.

Example

Enable the account locking function for administrators who fail remote authentication, and set the authentication retry interval to 5 minutes, maximum number of consecutive authentication failures to 3, and account locking period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] administrator remote authen-fail retry-interval 5 retry-time 3 block-time 5
```

13.1.21 admin-user privilege level

Function

The **admin-user privilege level** command configures a user as an administrator to log in to the device and sets the user privilege level.

The **undo admin-user privilege level** command cancels the default user privilege level.

By default, the user privilege level is not specified.

Format

admin-user privilege level *level*

undo admin-user privilege level

Parameters

Parameter	Description	Value
level	Specifies a user privilege level. A larger value indicates a higher user privilege level. After logging in to the device, a user can run only the commands at the same or lower privilege levels.	The value is an integer that ranges from 0 to 15.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device provides hierarchical management of commands. A command has a privilege level, and a user can run only the commands at the same or lower privilege levels. By using the **admin-user privilege level** command to set the user privilege level, the device controls commands used by users.

By default, commands are classified into the following privilege levels:

- Level 0 (visit level): Commands at level 0 include diagnosis commands such as ping and tracert commands and commands that are used to access a remote device such as the STelnet client. Commands at level 0 cannot be used to save configuration files.
- Level 1 (monitoring level): Commands at level 1 are used for system maintenance, including display commands. Commands at level 1 cannot be used to save configuration files.
- Level 2 (configuration level): Commands at level 2 are used for service configuration, including routing commands and commands at each network layer to provide network services for users.
- Level 3 (management level): Commands at level 3 are used for basic operations of the system to support services, including file system, FTP, Trivial File Transfer Protocol (TFTP), configuration file switching commands, slave board control commands, user management commands, command level configuration commands, and debugging commands.

To manage users in a refined manner, upgrade command privilege levels to levels 0 to 15. You can run the **command-privilege level** command to upgrade command privilege levels in a batch. You can also run the **command-privilege level rearrange** command to increase privilege levels.

- If non-authentication is used, the administrator privilege level is specified using the **user privilege** command in the VTY interface view.
- If local authentication is used, the user privilege level of the administrator is the local user privilege level configured using the **local-user privilege level** command.
- If remote authentication is performed, the administrator privilege level can be set in the following ways, in descending order of priority:
  a. Using the user privilege level sent by an authentication server to the device after authentication has succeeded
  b. Running the **admin-user privilege level** command to set the administrator privilege level in a service scheme
  c. Running the **user privilege** command to set the user privilege level in VTY mode
- If both remote authentication and local authentication are configured and remote authentication is performed before local authentication, the administrator privilege level is that used in remote authentication. If local authentication is performed because the remote server does not respond, the administrator privilege level is the local user privilege level configured using the **local-user privilege level** command.

The device can update the configuration in a domain dynamically. After a service scheme is applied to a domain, you can directly modify the user privilege level in

the service scheme but cannot unbind the service scheme from the domain. To delete the service scheme, run the **undo service-scheme (AAA domain view)** command.

Follow-up Procedure

Run the **display service-scheme** command to view the user privilege level in a service scheme.

Example

Configure a user as an administrator to log in to the device and set the administrator privilege level to 15.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme svcscheme1
[HUAWEI-aaa-service-svcscheme1] admin-user privilege level 15
```

13.1.22 assignment

Function

The **assignment** command configures the VLAN assignment algorithm in a VLAN pool.

The **undo assignment** command restores the default VLAN assignment algorithm in a VLAN pool.

By default, the VLAN assignment algorithm is **hash** in a VLAN pool.

Format

assignment { **even** | **hash** }

undo assignment

Parameters

Parameter	Description	Value
even	Sets the VLAN assignment algorithm to **even**.	-
hash	Sets the VLAN assignment algorithm to **hash**.	-

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When the VLAN assignment algorithm is set to **even**, service VLANs are assigned to users from the VLAN pool based on the order in which users go online. Address pools mapping the service VLANs evenly assign IP addresses to users. If a user goes online many times, it obtains different IP addresses.
- When the VLAN assignment algorithm is set to **hash**, VLANs are assigned to users from the VLAN pool based on the hash result of their MAC addresses. As long as the VLANs in the VLAN pool do not change, the users obtain fixed VLAN. A user is preferentially assigned the same IP address when going online at different times.

Precautions

For the **even** VLAN assignment algorithm, the aging time of IP addresses is set large on the DHCP server. A user is assigned different IP addresses when going online at different times. As a result, a user may occupy many IP addresses, which wastes IP addresses. Additionally, frequent IP address changes may lower user experience.

Configuration Impact

The VLAN assignment algorithm configuration affects only newly connected users, but not those that have been connected to the network.

Example

Set the VLAN assignment algorithm to **even** in the VLAN pool **test**.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] assignment even
```

13.1.23 authentication-mode (authentication scheme view)

Function

The **authentication-mode** command configures an authentication mode for an authentication scheme.

The **undo authentication-mode** command restores the default authentication mode in an authentication scheme.

By default, local authentication is used. The names of local users are case-insensitive.

Format

authentication-mode { **hwtacacs** | [**local** | **local-case**] | **radius** | **haca** } * [**none**]

authentication-mode none

undo authentication-mode

NOTE

Only the following switch models support HACA:

S200, S1730S-S1

S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H and S6720S-S

Parameters

Parameter	Description	Value
hwtacacs	Authenticates users using an HWTACACS server. To perform HWTACACS authentication, configure an HWTACACS authentication server in an HWTACACS server template.	-
local	Authenticates users locally and sets local user names to case-insensitive.	-
local-case	Authenticates users locally and sets local user names to case-sensitive.	-
radius	Authenticates users using a RADIUS server. To perform RADIUS authentication, configure a RADIUS authentication server in a RADIUS server template.	-
haca	Authenticates users using a Huawei Agile Cloud Authentication (HACA) server.	-
none	Indicates non-authentication. That is, users access the network without being authenticated.	-

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users, configure an authentication mode in an authentication scheme.

If multiple authentication modes are configured in an authentication scheme, the authentication modes are used according to the sequence in which they were configured.

- In the sequence of local authentication followed by remote authentication:

  If a login account is not created locally but exists on the remote server, the authentication mode is changed from local authentication to remote authentication.

  If a login account is created locally and on the remote server, and local authentication fails because the password is incorrect, remote authentication will not be performed.
- In the sequence of remote authentication followed by local authentication:

  If a login account is created locally but not on the remote server, remote authentication fails and local authentication will not be performed.

  A user is authenticated using the local authentication mode only when the remote server is Down or does not respond to the user's authentication request.

  NOTE

  Normally, if the remote server is Down or does not respond, local authentication is used. If a large number of users need to go online through the device, the device may be unable to process responses from the server in a timely manner. As a result, the AAA module of the device cannot receive responses from the server until the protection timer expires. These users then cannot go online and cannot be authenticated using local authentication. In this case, reconnect these offline users to the device.

You can configure multiple authentication modes in an authentication scheme to reduce authentication failure possibilities.

- After the **authentication-mode radius local** command is used, the device cannot complete RADIUS authentication if it fails to connect to the RADIUS authentication server. In this case, the device starts local authentication.
- After the **authentication-mode local radius** command is used, if the entered user name exists on the device but the entered password is incorrect, the user fails the authentication; if the entered user name does not exist on the device, the user is redirected to the RADIUS authentication mode and is authenticated based on user information on the RADIUS server.

NOTE

- When both RADIUS authentication and non-authentication are configured, if the user fails the RADIUS authentication, non-authentication cannot be used. As a result, a user fails to log in.
- If you run the **authentication-mode** command to configure non-authentication and run the **authentication-mode (user interface view)** command to configure AAA authentication, the device does not allow administrators to log in from the user interface view.
- If none authentication is configured or none authentication is configured as the backup authentication mode, you need to run the **accounting start-fail online** or **accounting-mode none** command in the accounting scheme view to prevent users from going offline due to accounting failures.

Precautions

If non-authentication is configured using the **authentication-mode** command, users can pass the authentication using any user name or password. Therefore, to protect the device and improve network security, you are advised to enable authentication, allowing only authenticated users to access the device or network.

It is not recommended that HACA authentication be configured together with another authentication (except non-authentication). Otherwise, the two configured authentication modes cannot take effect simultaneously. For example, if the **authentication-mode haca radius** command is configured, users can log in after passing HACA authentication; if users fail HACA authentication, RADIUS authentication will not be performed on them.

Example

Configure the authentication scheme named **scheme1** to use RADIUS authentication.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme scheme1
[HUAWEI-aaa-authen-scheme1] authentication-mode radius
```

13.1.24 authentication-scheme (AAA domain view)

Function

The **authentication-scheme** command applies an authentication scheme to a domain.

The **undo authentication-scheme** command restores the default configuration of the authentication scheme in a domain.

By default, the authentication scheme named **radius** is applied to the **default** domain, the authentication scheme named **default** is applied to the **default_admin** domain, and the authentication scheme named **radius** is applied to other domains.

Format

authentication-scheme *scheme-name*

undo authentication-scheme

Parameters

Parameter	Description	Value
scheme-name	Specifies the name of an authentication scheme.	The value must be an existing authentication scheme name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users in a domain, run the **authentication-scheme (AAA domain view)** command to apply an authentication scheme to a domain.

Prerequisites

An authentication scheme has been created and configured with required parameters, for example, the authentication mode and authentication mode for upgrading user levels.

Example

Apply the authentication scheme named **scheme1** to a domain named **domain1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain domain1
[HUAWEI-aaa-domain-domain1] authentication-scheme scheme1
```

13.1.25 authentication-scheme (AAA view)

Function

The **authentication-scheme** command creates an authentication scheme and displays its view.

The **undo authentication-scheme** command deletes an authentication scheme.

By default, the default authentication scheme is used. This default authentication scheme can be modified but cannot be deleted. In the default authentication scheme:

- Local authentication is used.
- The **offline** policy is used for authentication failures.

By default, the system also provides the authentication scheme **radius**. The **radius** authentication scheme can be modified, but cannot be deleted. In the **radius** authentication scheme:

- RADIUS authentication is used.
- The **offline** policy is used for authentication failures.

Format

authentication-scheme *scheme-name*

undo authentication-scheme *scheme-name*

Parameters

Parameter	Description	Value
scheme-name	Specifies the name of an authentication scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users, run the **authentication-scheme** command to create an authentication scheme. Creating an authentication scheme is necessary before performing authentication-relevant configurations.

Follow-up Procedure

After an authentication scheme is created, run the **authentication-mode (authentication scheme view)** command to configure an authentication mode in an authentication scheme.

After an authentication scheme is configured, run the **authentication-scheme (AAA domain view)** command to apply the authentication scheme to a domain.

Precautions

If the configured authentication scheme does not exist, the **authentication-scheme** command creates an authentication scheme and displays the authentication scheme view. If the configured authentication scheme already exists, the **authentication-scheme** command directly displays the authentication scheme view.

To delete an authentication scheme applied to a domain, run the **undo authentication-scheme (AAA domain view)** command.

Example

Create an authentication scheme named **newscheme**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme newscheme
[HUAWEI-aaa-authen-newscheme]
```

Access the default authentication scheme view.

```
<HUAWEI> system-view
[HUAWEI] aaa
```



```
[HUAWEI-aaa] authentication-scheme default
[HUAWEI-aaa-authen-default]
```

13.1.26 authentication-super

Function

The **authentication-super** command configures an authentication mode for upgrading user levels in an authentication scheme.

The **undo authentication-super** command restores the default authentication mode for upgrading user levels in an authentication scheme.

By default, the **super** mode is used. That is, local authentication is used.

Format

authentication-super { **hwtacacs** | **radius** | **super** } * [**none**]

authentication-super none

undo authentication-super

Parameters

Parameter	Description	Value
hwtacacs	Uses HWTACACS authentication to upgrade user levels.	-
radius	Uses RADIUS authentication to upgrade user levels.	-
super	Uses local authentication to upgrade user levels.	-
none	Indicates that user levels can be upgraded without authentication.	-

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If users in a domain need to upgrade their levels, the device requests the users to enter the password to authenticate the users. If AAA authentication has been configured using the **authentication-mode (user interface view)** command, run the **authentication-super** command to configure an authentication mode for upgrading user levels.

When you use the **super** command to switch a user level to a lower level or the same level, no authentication is required. When you use the **super** command to switch a user level to a higher level, authentication is required. The user can be granted rights only after being authenticated.

- If **super** is used and the local authentication is specified, run the **local-user** command in the AAA view to create a local user and set parameters for the local user.
- If **hwtacacs** is used and the HWTACACS authentication is specified, perform configurations relevant to HWTACACS authentication.
- If **radius** is used and the RADIUS authentication is specified, perform configurations relevant to RADIUS authentication.
- If **radius** is specified, the RADIUS authentication mode is used to upgrade the user level. The user name to be sent is $enab+user level. Ensure that the user has been configured on the server.
- If **none** is used, no authentication is required.

Precautions

If multiple authentication modes are configured in an authentication scheme, these authentication modes are used in the sequence in which they were configured. The device uses another authentication mode only when it does not receive any response in the current authentication. The device does not switch to another authentication mode if the user fails to pass one authentication mode.

Example

Set the authentication mode to HWTACACS authentication in the authentication scheme **scheme1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme scheme1
[HUAWEI-aaa-authen-scheme1] authentication-super hwtacacs
```

13.1.27 authentication-type radius chap access-type admin

Function

The **authentication-type radius chap access-type admin** command replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators.

The **undo authentication-type radius chap access-type admin** command restores PAP authentication when RADIUS authentication is performed on administrators.

By default, PAP authentication is used when RADIUS authentication is performed on administrators.

Format

authentication-type radius chap access-type admin [**ftp** | **ssh** | **telnet** | **terminal** | **http**] *

undo authentication-type radius chap access-type admin

Parameters

Parameter	Description	Value
ftp	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using FTP.	-
ssh	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using SSH.	-
telnet	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using Telnet.	-
terminal	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using a terminal.	-

Parameter	Description	Value
http	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using a web management system.	-

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

CHAP is ciphertext authentication protocol. During CHAP authentication, the NAS device sends the user name, encrypted password, and 16-byte random code to the RADIUS server. The RADIUS server searches for the database according to the user name and obtains the password that is the same as the encrypted password at the user side. The RADIUS server then encrypts the received 16-byte random code and compares the result with the password. If they are the same, the user is authenticated. If they are different, the user fails to be authenticated. In addition, if the user is authenticated, the RADIUS server generates a 16-byte random code to challenge the user. CHAP is more secure and reliable than PAP.

If no parameter is specified when you run the **authentication-type radius chap access-type admin** command, the configuration takes effect on the administrators who access the device using FTP, SSH, Telnet, Terminal, and HTTP.

When the device is connected to the RADIUS server that supports CHAP authentication, this function needs to be configured.

Example

Replace PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using FTP.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme scheme1
[HUAWEI-aaa-authen-scheme1] authentication-type radius chap access-type admin ftp
```


13.1.28 authorization-cmd

Function

The **authorization-cmd** command configures command-specific authorization for an administrator of a specific level. After command-specific authorization is enabled and an administrator of a specific privilege level logs in to the device, the commands that the administrator enters can be executed only after being authorized by the HWTACACS server.

The **undo authorization-cmd** command disables command-specific authorization for an administrator of a specific privilege level.

By default, the command-specific authorization is disabled. That is, an administrator of any level can execute only commands of or below its privilege level after logging in to the device.

Format

authorization-cmd *privilege-level* **hwtacacs** [**local**] [**none**]

undo authorization-cmd *privilege-level*

Parameters

Parameter	Description	Value
privilege-level	Specified the administrator privilege level.	The value is an integer that ranges from 0 to 15.
hwtacacs	Indicates HWTACACS authorization.	-
local	Indicates local authorization.	-
none	Indicates that command line authorization is directly performed for a user if the HWTACACS server does not respond to the authorization request of the user.	-

Views

Authorization scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After being authorized, the users at a certain privilege level can run the commands of the same or lower privilege levels. Command line authorization can be configured to implement minimum user rights control. When command line authorization is enabled, each command entered by users can be executed only after being authorized. After command line authorization is enabled for users at a certain privilege level, the commands run by the users at that privilege level must be authorized by an HWTACACS server.

Precautions

- You are advised to configure local authorization as a backup of command line authorization. If command line authorization cannot be performed because of a failure on an HWTACACS server, the device starts local authorization.
- After the **authorization-cmd** command is executed, command line authorization does not take effect immediately. Command line authorization takes effect only when an authorization scheme containing command line authorization is applied to administrator view correctly.
- Commands whose privilege levels are higher than the administrator privilege level cannot be authorized and fail to be executed.
- When configuring the **authorization-cmd** *privilege-level* **hwtacacs local** command, you must create a local account. The device then performs authentication based on the local account configuration.

NOTICE

After an authorization scheme containing command line authorization is applied to administrator view, if you run the **undo authorization-cmd** command, an online administrator at a certain privilege level cannot run any commands except for the **quit** command. The administrator needs to log in again.

Example

Configure command line authorization for administrators at the privilege level 2.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme scheme1
[HUAWEI-aaa-author-scheme1] authorization-cmd 2 hwtacacs
```

13.1.29 authorization-info check-fail policy

Function

The **authorization-info check-fail policy** command determines whether the device allows users to go online after the authorization information check fails.

The **undo authorization-info check-fail policy** command restores the default configuration.

By default, the device allows users to go online after the authorization information check fails.

Format

authorization-info check-fail policy { **online** | **offline** }

undo authorization-info check-fail policy

Parameters

Parameter	Description	Value
online	Indicates that the device allows users to go online after the authorization information check fails.	-
offline	Indicates that the device prohibits users from going online after the authorization information check fails.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device supports user authorization through the ACL, UCL Group, User Group and VLAN delivered from the RADIUS server. If the ACL, UCL Group, User Group and VLAN delivered from the RADIUS server are not configured on the device, the authorization information check fails on the device.

You can use this command to configure the users to go online and the authorization information delivered by the RADIUS server does not take effect.

Example

Configure the device to allow users to go online after the authorization information check fails.

```
<HUAWEI> system-view
[HUAWEI] authorization-info check-fail policy online
```

13.1.30 authorization-mode

Function

The **authorization-mode** command configures an authorization mode for an authorization scheme.

The **undo authorization-mode** command restores the default authorization mode in an authorization scheme.

By default, local authorization is used. The names of local users are case-insensitive.

Format

authorization-mode { **hwtacacs** | **if-authenticated** | { **local** | **local-case** } } * [**none**]

authorization-mode none

undo authorization-mode

Parameters

Parameter	Description	Value
hwtacacs	Indicates that the user is authorized by an HWTACACS server.	-
if-authenticated	Indicates that only the user who succeeds in authentication is authorized. The configuration of if-authenticated authorization does not take effect in RADIUS authentication.	-
local	Authenticates users locally and sets local user names to case-insensitive.	-
local-case	Authenticates users locally and sets local user names to case-sensitive.	-
none	Indicates non-authorization.	-

Views

Authorization scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authorize users, configure an authorization mode in an authorization scheme.

You can configure multiple authorization modes in an authorization scheme to reduce the chance of authorization failures.

After the **authorization-mode hwtacacs local** command is used, if it fails to connect to the HWTACACS authentication server and HWTACACS authorization cannot be performed, the device starts local authorization.

Precautions

- If multiple authorization modes are used in an authorization scheme, the **if-authenticated** mode or **none** mode must be used as the last authorization mode.
- If the authorization mode is set to **if-authenticated** or **none**, the local authentication administrator does not inherit the level configured using the **local-user privilege level** command after login. The administrator first inherits the level configured using the **admin-user privilege level** command in the service scheme bound to the domain. If the level is not configured in the domain, the administrator inherits the level configured using the **user privilege** command in the VTY view.

  By default, users who log in to a device in the VTY view of the console interface are at level 15 and users who log in to a device in other VTY views are at level 0.
- If multiple authorization modes are configured in an authorization scheme, the authorization modes are used according to the sequence in which they were configured. The device uses another authorization mode only when it does not receive any response in the current authorization mode.

Example

Configure the authorization scheme named **scheme1** to apply HWTACACS authorization.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme scheme1
[HUAWEI-aaa-author-scheme1] authorization-mode hwtacacs
```

13.1.31 authorization-modify mode

Function

The **authorization-modify mode** command configures the update mode for user authorization information delivered by the authorization server.

The **undo authorization-modify mode** command restores the default update mode for user authorization information delivered by the authorization server.

By default, the update mode of user authorization information delivered by the authorization server is **overlay**. That is, the new user authorization information overwrites all existing user authorization information.

Format

authorization-modify mode { **modify** | **overlay** }

undo authorization-modify mode

Parameters

Parameter	Description	Value
modify	Indicates the **modify** mode.	-
overlay	Indicates the **overlay** mode.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

The authorization server can deliver all or part of user authorization information, such as the ACL rule and dynamic VLAN.

You can run the **authorization-modify mode** command to configure one of the following update modes for user authorization information delivered by the authorization server:

- **modify**: modification mode indicating that new user authorization information overwrites only existing user authorization information of the same type.
- **overlay**: overwriting mode indicating that new user authorization information overwrites all existing user authorization information.

If the authorization server has delivered ACL 3001 to a user, and the administrator needs to deliver new authorization information:

- In the **modify** mode, if the new authorization information is ACL 3002, the authorization information of the user is ACL 3002. If the new authorization information is VLAN 100, the authorization information of the user is ACL 3001 and VLAN 100.
- In the **overlay** mode, no matter whether the new authorization information is ACL 3002 or VLAN 100, the authorization information of the user is the new ACL or VLAN.

This command takes effect for only the authorization information delivered by the RADIUS server.

After a user group or service scheme is authorized to a user on the device and a certain attribute configured in the user group or service scheme is modified on the

server, if other configured attributes need to be modified, the authorization information on the server must contain the previously modified attribute. Otherwise, the original attribute value in the user group or service scheme will be restored. For example, to modify an attribute in a user group:

1. The device authorizes the user group configured with the VLAN and ACL attributes to a user.
2. To modify the VLAN attribute, authorize the new VLAN attribute to the user through the RADIUS server.
3. To modify the ACL attribute after the VLAN attribute is modified, you must authorize the modified VLAN attribute and new ACL attribute through the RADIUS server. Otherwise, the original VLAN attribute in the user group will be restored.

NOTE

For user re-authentication:

- If the Session-Timeout attribute is delivered during RADIUS CoA authorization, the original re-authentication timer is deleted and the timer carried by the Session-Timeout attribute is started.
- If the Session-Timeout attribute is not delivered during RADIUS CoA authorization:
  - When the **modify** mode is used, the original re-authentication timer is not deleted; instead, the timer is suspended during user authorization and continues to take effect after the authorization completes.
  - When the **overlay** mode is used:

    If the original re-authentication timer is locally configured, the original re-authentication timer is not deleted; instead, the timer is suspended during user authorization and continues to take effect after the authorization completes.

    If the original timer is delivered by the server, the original timer is deleted and re-authentication is performed depending on whether the local re-authentication timer is configured on the device.

Example

Set the update mode of user authorization information delivered by the authorization server to **modify**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-modify mode modify
```

13.1.32 authorization-scheme (AAA domain view)

Function

The **authorization-scheme** command applies an authorization scheme to a domain.

The **undo authorization-scheme** command unbinds an authorization scheme from a domain.

By default, no authorization scheme is applied to a domain.

Format

authorization-scheme *authorization-scheme-name*

undo authorization-scheme

Parameters

Parameter	Description	Value
authorization-scheme-name	Specifies the name of an authorization scheme.	The authorization scheme must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

RADIUS integrates authentication and authorization; therefore, RADIUS authorization and authentication must be used together. HWTACACS separates authentication from authorization; therefore, you can configure another authorization type even if HWTACACS authentication, local authentication, or non-authentication is used.

To authorize users in a domain, run the **authorization-scheme (AAA domain view)** command.

Prerequisites

An authorization scheme has been created and configured with required parameters, for example, the authorization mode and command line authorization.

Example

Apply the authorization scheme **author1** to the domain **isp1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme author1
[HUAWEI-aaa-author-author1] quit
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] authorization-scheme author1
```

13.1.33 authorization-scheme (AAA view)

Function

The **authorization-scheme** command creates an authorization scheme and enters the authorization scheme view, or directly enters an existing authorization scheme view.

The **undo authorization-scheme** command deletes an authorization scheme.

By default, the default authorization scheme is used. This default authorization scheme can be modified but cannot be deleted. In the default authorization scheme, local authorization is used and command line authorization is disabled.

Format

authorization-scheme *authorization-scheme-name*

undo authorization-scheme *authorization-scheme-name*

Parameters

Parameter	Description	Value
authorization-scheme-name	Specifies the name of an authorization scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

RADIUS integrates authentication and authorization; therefore, RADIUS authorization and authentication must be used together. HWTACACS separates authentication from authorization; therefore, you can configure another authorization type even if HWTACACS authentication, local authentication, or non-authentication is used. You must run the **authorization-scheme** command to create an authorization scheme before performing authorization-relevant configurations, for example, setting the authorization mode and command line authorization function.

Follow-up Procedure

After an authorization scheme is created:

- Run the **authorization-mode** command to configure an authorization mode in an authorization scheme.
- Run the **authorization-cmd** command to configure command line authorization for users at a certain level.

After an authorization scheme is configured, run the **authorization-scheme (AAA domain view)** command to apply the authorization scheme to a domain.

Precautions

- If the configured authorization scheme does not exist, the **authorization-scheme (AAA view)** command creates an authorization scheme and displays the authorization scheme view.
- If the configured authorization scheme already exists, the **authorization-scheme (AAA view)** command directly displays the authorization scheme view.

To delete the authorization scheme applied to a domain, run the **undo authorization-scheme (AAA domain view)** command.

Example

Create an authorization scheme named **scheme0**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme scheme0
[HUAWEI-aaa-author-scheme0]
```

Enter the default authorization scheme view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme default
[HUAWEI-aaa-author-default]
```

13.1.34 cmd recording-scheme

Function

The **cmd recording-scheme** command applies a policy in a recording scheme to record the commands executed on the device.

The **undo cmd recording-scheme** command deletes a policy from a recording scheme.

By default, the commands that are used on the device are not recorded.

Format

cmd recording-scheme *recording-scheme-name*

undo cmd recording-scheme

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During the device configuration, incorrect operations may result in network faults. After the **cmd recording-scheme** command is executed, you can view records of the commands executed on the device to locate the network faults.

Prerequisites

A recording scheme has been created by using the **recording-scheme** command and a recording mode has been configured by using the **recording-mode hwtacacs** command.

Example

Configure a policy in the recording scheme **scheme0** to record the commands executed on the device.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template hw1
[HUAWEI-hwtacacs-hw1] quit
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme0
[HUAWEI-aaa-recording-scheme0] recording-mode hwtacacs hw1
[HUAWEI-aaa-recording-scheme0] quit
[HUAWEI-aaa] cmd recording-scheme scheme0
```

13.1.35 cut access-user

Function

The **cut access-user** command terminates one or multiple access user connections, also forcibly disconnecting online users.

Format

cut access-user { **domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **mac-address** *mac-address* | **service-scheme** *service-scheme-name* | **access-slot** *slot-id* | **user-id** *begin-number* [*end-number*] | **username** *user-name* }

cut access-user ssid *ssid-name* (This command is only supported by the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.)

cut access-user access-type admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**] [**username** *user-name*]

Parameters

Parameter	Description	Value
domain *domain-name*	Disconnects sessions in a specified domain.	The value must be the name of an existing domain.
interface *interface-type interface-number*	Disconnects sessions on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
vlan *vlan-id* [**qinq** *qinq-vlan-id*]	Disconnects sessions in a specified VLAN. • *vlan-id* specifies the ID of a VLAN. In QinQ applications, this parameter specifies the inner VLAN ID. • *qinq-vlan-id* specifies the outer VLAN ID.	The values of *vlan-id* and *qinq-vlan-id* are integers that range from 1 to 4094.
ip-address *ip-address*	Disconnects sessions initiated by a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value must be an existing VPN instance name.
mac-address *mac-address*	Disconnects sessions initiated by a specified MAC address.	The value is in H-H-H format. An H contains 4 hexadecimal digits.
service-scheme *service-scheme-name*	Terminates connections based on the service scheme.	The value must be the name of an existing service scheme.
access-slot *slot-id*	Disconnects sessions on a specified device.	The value range depends on the model of the device.
ssid *ssid-name*	Disconnects sessions initiated by a service set identifier (SSID) for a service set.	The SSID must already exist. **NOTE** SSID is supported only in the NAC unified mode.
user-id *begin-number* [*end-number*]	Disconnects sessions of a specified user.	The user-id must exist on the device.

Parameter	Description	Value
username *user-name*	Disconnects sessions of a user with a specified user name.	The value must be the name of an existing user.
access-type	Displays information about the users using the specified authentication mode.	-
admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**]	Displays information about the administrators using the specified authentication mode. • **ftp**: FTP user • **ssh**: SSH user • **telnet**: Telnet user • **terminal**: Terminal user • **web**: Web user	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Performing some configurations, such as AAA, on the device, requires that no users be online. You can run the **cut access-user** command to disconnect sessions.

Precautions

- The **cut access-user** command interrupts all services of the user whose session is torn down.
- For administrators, lower-level users cannot tear down the connections of higher-level users.
- If the character string of the user name contains spaces (for example, a b), you can run the **display access-user username "a b"** command to view online users.
- If the character string of the user name contains spaces and quotation marks ("") simultaneously, you cannot use the user name to view online users. In this case, you can run the **display access-user | include** *username* command to view the user ID of the online user, and then run the **display access-user**

user-id *user-id* command to view the user. Alternatively, you can run the **cut access-user user-id** *user-id* command to force the user to go offline.

Example

Tear down the session initiated by the IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] cut access-user ip-address 10.1.1.1
```

13.1.36 display aaa

Function

The **display aaa** command displays information about normal logout, abnormal logout, and login failures.

Format

display aaa { **offline-record** | **abnormal-offline-record** | **online-fail-record** } { **all** | **reverse-order** | **domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **mac-address** *mac-address* | **access-slot** *slot-number* | **time** *start-time end-time* [**date** *start-date end-date*] | **username** *user-name* [**time** *start-time end-time* [**date** *start-date end-date*]] } [**brief**]

Parameters

Parameter	Description	Value
offline-record	Displays normal logout records.	-
abnormal-offline-record	Displays abnormal logout records.	-
online-fail-record	Displays login failure records.	-
all	Displays all login and logout records.	-
reverse-order	Displays the records in order of newest to oldest.	-
domain *domain-name*	Specifies the name of a domain.	The value is a string of 1 to 64 case-insensitive characters, excluding spaces, *, ?, and ".
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Parameter	Description	Value
vlan *vlan-id*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.
qinq *qinq-vlan-id*	Specifies the outer VLAN ID.	The value is an integer that ranges from 1 to 4094.
ip-address *ip-address*	Specifies an IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
mac-address *mac-address*	Specifies a MAC address.	The value is in H-H-H format. An H is a 4-digit hexadecimal number.
access-slot *slot-number*	Specifies a slot ID.	The value is an integer. The value range depends on the model of the device.
username *user-name*	Specifies a user.	The value must be an existing user.
time *start-time end-time*	Specifies a time range.	The format is HH:MM:SS, indicating hour:minute:second.
date *start-date end-date*	Specifies a date.	The format is YYYY/MM/DD. YYYY is the year, MM is the month, and DD is the day.
brief	Displays brief login and logout information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command allows you to view information about user normal logouts, abnormal logouts, and login failures based on the domain name, interface, IP address, VPN instance, MAC address, or slot ID.

Precautions

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

NOTE

For the meanings, causes, and handling suggestions of abnormal user logins and logouts, see "**Common Causes of Access Authentication**" in the *Huawei S Series Campus Switches Troubleshooting Guide*.

Example

Display information about normal user logouts in the domain **rds**.

```
<HUAWEI> display aaa offline-record domain rds
 ------------------------------------------------------------------------
 User name             : test@rds
 Domain name           : rds
 User MAC              : 00e0-fc01-b67c
 User access type      : 802.1x
 User access interface : Wlan-Dbss1
 Qinq vlan/User vlan   : 0/1
 User IP address       : 192.168.2.2
 User IPV6 address     : -
 User ID               : 19
 User login time       : 2008/10/01 04:49:39
 User offline time     : 2008/10/01 04:59:43
 User offline reason   : EAPOL user request
 User name to server   : test@rds
 AP ID                 : 0
 Radio ID              : 0
 AP MAC                : b001-0000-ac01
 SSID                  : ssid1
 ------------------------------------------------------------------------
 Are you sure to display some information?(y/n)[y]:
```

Display all unexpected user logout records.

```
<HUAWEI> display aaa abnormal-offline-record all
 ------------------------------------------------------------------------------
 User name             : cdw
 Domain name           : l2bng
 User MAC              : 00e0-fc01-4f2b
 User access type      : MAC
 User access interface : Wlan-Dbss1
 Qinq vlan/User vlan   : 0/2012
 User IP address       : 10.17.17.219
 User IPV6 address     : -
 User ID               : 18
 User login time       : 2017/03/16 19:40:18
 User offline time     : 2017/03/16 19:43:20
 User offline reason   : AAA cut command
 User name to server   : cdw@l2bng
 AP ID                 : 1
 Radio ID              : 0
 AP MAC                : 00e0-fc01-ac01
 SSID                  : ssid1
```



```
  ---------------------------------------------------------------------------
  Are you sure to display some information?(y/n)[y]:
```

Display brief information about unexpected user logout records.

```
<HUAWEI> display aaa abnormal-offline-record all brief
  ---------------------------------------------------------------------------
  UserID    Username                  IP address      MAC
Reason
            SSID                                  User offline time

-------------------------------------------------------------------------------------------

  16010     zcm                       10.1.2.10   -                   Idle cut
            -                                     2022/05/09 14:55:47

-------------------------------------------------------------------------------------------

  Total: 1,Printed: 1
```

Display online failure information of all users.

```
<HUAWEI> display aaa online-fail-record all
  ---------------------------------------------------------------------------
  User name              : test
  Domain name            : default
  User MAC               : 00e0-fc01-85bc
  User access type       : MAC
  User access interface  : Eth-Trunk10
  Qinq vlan/User vlan    : 116/100
  User IP address        : 10.1.1.10
  User IPV6 address      : -
  User ID                : 326678
  User login time        : 2019/09/20 10:06:32
  User online fail reason : Radius authentication reject
  Authen reply message   : ErrorReason is The access quanti...
  User name to server    : zxx
  ---------------------------------------------------------------------------
  Are you sure to display some information?(y/n)[y]:
```

Display information about user login failures. In this example, the login failure cause is IP address conflict.

```
<HUAWEI> display aaa online-fail-record mac-address 00e0-fc01-85bc
  ---------------------------------------------------------------------------
  User name              : test
  Domain name            : default
  User MAC               : 00e0-fc01-85bc
  User access type       : None
  User access interface  : Eth-Trunk10
  Qinq vlan/User vlan    : 116/100
  User IP address        : -
  Conflict IP address    : 192.168.10.1
  User IPV6 address      : -
  User ID                : 326678
  User login time        : 2020/09/20 10:06:32
  User online fail reason : IP address conflict
  Authen reply message   : -
  ---------------------------------------------------------------------------
  Are you sure to display some information?(y/n)[y]:
```

Table 13-2 Description of the **display aaa** command output

Item	Description
User name	User name.
Domain name	Domain of a user.

Item	Description
User MAC or MAC	MAC address of a user.
User access type	Access type of a user: ● 802.1x indicates that the user accesses the network through 802.1X. ● API indicates that the user accesses the network through the API. ● FTP indicates that the user accesses the network through FTP. ● Telnet indicates that the user accesses the network through Telnet. ● Terminal indicates that the user accesses the network through terminal. ● SSH indicates that the user accesses the network through SSH. ● x25-pad indicates that the user accesses the network through x25-pad. ● HTTP indicates that the user accesses the network through HTTP. ● Web indicates that the user accesses the network through web. For the related command, see **local-user service-type**.
User access interface	Access interface of a user.
Qinq vlan/User vlan	VLAN that a user belongs to. ● In QinQ application, QinQvlan indicates the outer VLAN ID and Uservlan indicates the inner VLAN ID. ● For a common VLAN, Uservlan indicates the VLAN ID, and QinQvlan is 0.
User IP address or IP address	IP address of a user.
User IPV6 address	IPv6 address of a user.
User ID	Index of a user.
User login time	Time when a user goes online.
User offline time	Time when a user goes offline.

Item	Description
User offline reason, User online fail reason, or Reason	Reason why a user fails to go online or offline. The common reasons are as follows: ● The value "EAPOL user request" indicates that an 802.1X user requests to go offline. ● The value "PPP user request" indicates that a PPP user requests to go offline. ● The value "Web user request" indicates that a web user requests to go offline. ● The value "AAA cut command" indicates that a user is deleted using command line. ● The value "Session time out" indicates that a session times out. ● The value "Idle cut" indicates that a user is disconnected because the user does not perform any operation within a specified period. ● The value "PPP authentication fail" indicates a PPP authentication failure. ● The value "STA disassociation" indicates that a STA is disassociated. ● The value "STA disassociation(delay offline)" indicates that the STA disassociation is delayed. ● The value "console reset or disable port" indicates that the management interface is Down. ● The value "Interface net down" indicates that an interface is Down. ● The value "Local authentication reject" indicates that the local authentication password is incorrect. ● The value "AS detect fail" indicates that an AS detection failure occurs on an access device in the policy association scenario. ● The value "AS smooth fail" indicates that an AS smoothing

Item	Description
	failure occurs on an access device in the policy association scenario. ● The value "AS configuration changed on interface" indicates that the user goes offline because the configuration of an AS interface on an access device changes in the policy association scenario. ● The value "IP address conflict" indicates that IP addresses conflict. ● The value "Add FPI item timeout(LPU)" indicates that the LPU authorization times out. ● The value "EAPOL client timeout" indicates that the client times out to respond. ● The value "low RSSI" indicates that the wireless signal strength is weak. ● The value "No authentication server configured" indicates that no authentication server is configured. ● The value "No radius-server template bound" indicates that no RADIUS server template is bound. ● The value "No tacacs-server template bound" indicates that no TACACS server template is bound. ● The value "No accounting server configured" indicates that no accounting server is configured. ● The value "Accounting server no response" indicates that the accounting server does not respond. ● The value "EAPOL client restart associate" indicates that the 802.1X client re-triggers an association. ● The value "Users with low priorities go offline" indicates that users go offline because their priorities are low. ● The value "Resources are insufficient" indicates that

Item	Description
	resources of the device are insufficient. • The value "Local Authentication user block" indicates that the local user is locked. • The value "Roaming is prohibited" indicates that user roaming is forbidden. • The value "AP fault" indicates that a wireless user is forced offline due to AP disconnection. • The value "Remote user is blocked" indicates that the remotely authenticated user is locked. • The value "Not support authorization with car" indicates that upstream CAR authorization is not supported for the user group. • The value "Not support authorization with user-group" indicates that re-mark authorization is not supported for the user group. • The value "Radius authentication reject" indicates that the RADIUS server responds with an Access-Reject packet. • The value "Data flow or online time exceed threshold" indicates that the online duration or used traffic of the user reaches the threshold. • The value "AS access interface down" indicates that the interface connecting an access device to a user goes Down in an SVF or policy association scenario. • The value "Server response times out" indicates that the server does not respond due to timeout. • The value "The shared keys on the device and Portal server are different" indicates that the shared key configured on the device is different from that configured on the Portal server.

Item	Description
	• "The acl locally delivered by AAA is invalid or does not exist": The ACL delivered by AAA is invalid or does not exist. • "The description of the acl sent by Radius is incorrect": The description of the ACL delivered by RADIUS is incorrect. • "The Rediect ACL delivered by AAA is incorrectly checked": The redirect ACL delivered by AAA is incorrect. • "AAA gets service scheme error": AAA failed to obtain SERVICE_SCHEME. • "AAA get author info error": AAA failed to obtain authentication information. • "AAA check author vlan error": AAA failed to check the authorized VLAN. • The value "AAA authorization dynamic vlan error" indicates that the dynamic VLAN authorized by AAA is incorrect. • The value "SAM failed to deliver authorized VLAN" indicates that SAM failed to deliver the authorized VLAN. • "SAM failed to deliver QOS": SAM failed to deliver QoS. • "SAM failed to deliver port mac limit": SAM failed to deliver the port MAC limit. • "SAM failed to deliver vm car": SAM failed to deliver VM CAR. • "User flow detect fail": User traffic detection fails.

Item	Description
Authen reply message	Authentication response message. If the Access-Reject packet returned by the RADIUS server carries this field, this field is filled with the message carried in the Access-Reject packet. The length of this field cannot exceed 32 bytes. Otherwise, the message "Authentication fail,user is blocked" or "Authentication fail" is displayed.
User name to server	User name sent by the device to the server.
AP ID	ID of the AP that a wireless user associates with.
Radio ID	ID of the radio that a wireless user associates with.
AP MAC	MAC address of the AP that a wireless user associates with.
SSID	SSID that a wireless user associates with.
Conflict IP address/Conflict IPv6 address	Conflicting IPv4 or IPv6 address.

13.1.37 display aaa configuration

Function

The **display aaa configuration** command displays the AAA configurations, for example, the domain, authentication scheme, authorization scheme, and accounting scheme.

Format

display aaa configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

AAA configurations are limited by system specifications. Before performing AAA configurations, run the **display aaa configuration** command to check whether there are sufficient resources.

Example

Display the AAA summary.

```
<HUAWEI> display aaa configuration
  Domain Name Delimiter                  : @
  Domainname parse direction             : Left to right
  Domainname location                    : After-delimiter
  Administrator user default domain      : default_admin
  Normal user default domain             : default
  Domain                                 : total: 32      used: 5
  Authentication-scheme                  : total: 33      used: 4
  Accounting-scheme                      : total: 32      used: 3
  Authorization-scheme                   : total: 32      used: 2
  Service-scheme                         : total: 32      used: 0
  Recording-scheme                       : total: 64      used: 0
  Local-user                             : total: 1000    used: 1
  Local-user block retry-interval        : 5 Min(s)
  Local-user block retry-time            : 3
  Local-user block time                  : 5 Min(s)
  Remote-admin-user block retry-interval : 5 Min(s)
  Remote-admin-user block retry-time     : 30
  Remote-admin-user block time           : 5 Min(s)
  Session timeout invalid enable         : No
  Navigator first login state            : No
```

Table 13-3 Description of the **display aaa configuration** command output

Item	Description
Domain Name Delimiter	Domain name delimiter, which can be any of the following characters: \ / : < > | @ ' %. The default domain name delimiter is @. To configure a domain name delimiter, run the **domain-name-delimiter** command.
Domain	Number of domains. • total: indicates the total number of domains that can be created. • used: indicates the number of domains that have been created.
Domainname parse direction	Parsing direction of the domain name. • Left to right • Right to left To configure this parameter, run the **domainname-parse-direction** command.

Item	Description
Domainname location	Domain name location. ● After-delimiter: The domain name is placed behind the domain name delimiter. ● Before-delimiter: The domain name is placed before the domain name delimiter. To configure this parameter, run the **domain-location** command.
Administrator user default domain	Domain name of administrator users.
Normal user default domain	Domain name of normal users.
Authentication-scheme	Number of authentication schemes. ● total: indicates the total number of authentication schemes that can be created. ● used: indicates the number of authentication schemes that have been created.
Accounting-scheme	Number of accounting schemes. ● total: indicates the total number of accounting schemes that can be created. ● used: indicates the number of accounting schemes that have been created.
Authorization-scheme	Number of authorization schemes. ● total: indicates the total number of authorization schemes that can be created. ● used: indicates the number of authorization schemes that have been created.
Service-scheme	Number of service schemes. ● total: indicates the total number of service schemes that can be created. ● used: indicates the number of service schemes that have been created.
Recording-scheme	Number of recording schemes. ● total: indicates the total number of recording schemes that can be created. ● used: indicates the number of recording schemes that have been created.

Item	Description
Local-user	Number of local users. • total: indicates the total number of local users that can be created. • used: indicates the number of local users that have been created.
Local-user block retry-interval	Authentication retry interval of a local account. To configure this parameter, run the **local-aaa-user wrong-password** command.
Local-user block retry-time	Maximum number of consecutive authentication failures for a local account. To configure this parameter, run the **local-aaa-user wrong-password** command.
Local-user block time	Locking time of a local account. To configure this parameter, run the **local-aaa-user wrong-password** command.
Remote-access-user block retry-interval	Authentication retry interval for access users who fail remote authentication. To configure this parameter, run the **access-user remote authen-fail** command.
Remote-access-user block retry-time	Maximum number of consecutive authentication failures for access users. To configure this parameter, run the **access-user remote authen-fail** command.
Remote-access-user block time	Locking time for access users who fail remote authentication. To configure this parameter, run the **access-user remote authen-fail** command.
Remote-admin-user block retry-interval	Authentication retry interval for administrators who fail remote authentication. To configure this parameter, run the **administrator remote authen-fail** command.
Remote-admin-user block retry-time	Maximum number of consecutive authentication failures for administrator. To configure this parameter, run the **administrator remote authen-fail** command.
Remote-admin-user block time	Locking period for administrators who fail remote authentication. To configure this parameter, run the **administrator remote authen-fail** command.

Item	Description
Session timeout invalid enable	• Yes: The device will not disconnect or reauthenticate users when the RADIUS server delivers session-timeout with value 0. • No: The device will disconnect or reauthenticate users when the RADIUS server delivers session-timeout with value 0. To configure this parameter, run the **aaa-author session-timeout invalid-value enable** command.
Navigator first login state	Indicates the first login status of the factory device.

13.1.38 display aaa statistics offline-reason

Function

The **display aaa statistics offline-reason** command displays the reasons why users go offline.

Format

display aaa statistics offline-reason

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display aaa statistics offline-reason** command helps you know the reason why a user goes offline. You can locate network faults according to the command output.

Example

Display reasons why users go offline.

```
<HUAWEI> display aaa statistics offline-reason
  19  User request to offline                                  :2
  87  AAA cut command                                          :1
```


Table 13-4 Description of the display aaa statistics offline-reason command output

Item	Description
19/87	Reason code.
User request to offline	A user requested to go offline.
2/1	Number of times users go offline.
AAA cut command	A user is disconnected by the **cut access-user** command.

13.1.39 display aaa-quiet administrator except-list

Function

The **display aaa-quiet administrator except-list** command displays IP addresses that a user can use to access the network when the user account is locked.

Format

display aaa-quiet administrator except-list

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After a user is configured to access the network using a specified IP address when the user account is locked using the **aaa-quiet administrator except-list** command, you can run the **display aaa-quiet administrator except-list** command to check information about the specified IP addresses.

Example

Display IP addresses that a user can use to access the network when the user account is locked.

```
<HUAWEI> display aaa-quiet administrator except-list
--------------------------------------------------------------------------------
Admin silent whitelist
--------------------------------------------------------------------------------
```



```
10.2.2.1
10.2.2.2
------------------------------------------------------------------------------
Total: 2, printed: 2
```

Table 13-5 Description of the **display aaa-quiet administrator except-list** command output

Item	Description
Admin silent whitelist	IP addresses configured in a whitelist.

13.1.40 display access-user (all views)

Function

The **display access-user** command displays information about online users (including access users and administrators).

Format

display access-user [**domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **ipv6-address** *ipv6-address* | **access-slot** *slot-id* | **wired** | **wireless**] [**detail**]

display access-user username *user-name* [**detail**]

display access-user ssid *ssid-name* (This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.)

display access-user [**mac-address** *mac-address* | **service-scheme** *service-scheme-name* | **user-id** *user-id*]

display access-user statistics

display access-user access-type admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**] [**username** *user-name*]

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **wireless** parameter.

Parameters

Parameter	Description	Value
domain *domain-name*	Displays information about users in a specified domain.	The domain name must already exist.

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about users on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
vlan *vlan-id* [**qinq** *qinq-vlan-id*]	Displays information about users in a VLAN. • *vlan-id* specifies the ID of a VLAN. In QinQ applications, this parameter specifies the inner VLAN ID. • *qinq-vlan-id* specifies the outer VLAN ID. In the authorized ISP VLAN scenario, you can view the user information only when the specified VLAN ID is the ISP VLAN ID.	The values of *vlan-id* and *qinq-vlan-id* are integers that range from 1 to 4094.
ip-address *ip-address*	Displays information about the user with a specified IP address. **NOTE** For NAC or static users, details about the users are displayed. For other users, brief information about the users is displayed.	The value of *ip-address* is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value must be an existing VPN instance name.
ipv6-address *ipv6-address*	Displays information about the user with a specified IPv6 address.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal digits in the format X:X:X:X:X:X:X:X.
mac-address *mac-address*	Displays information about the user with a specified MAC address.	The value is in H-H-H format. An H contains four hexadecimal digits.

Parameter	Description	Value
service-scheme *service-scheme-name*	Displays information about the user with a specified service scheme.	The service scheme must already exist.
access-slot *slot-id*	Displays information about users connecting to a specified device.	The value range depends on the model of the device.
ssid *ssid-name*	Specifies the SSID for a service set.	The SSID must already exist. **NOTE** SSID is supported only in the NAC unified mode.
username *user-name*	Displays information about the user with a user name.	The user name must already exist.
statistics	Displays user statistics on the device. • Historical wireless user statistics: displays historical wireless user statistics on the device. • Current online user statistics: displays current user statistics on the device.	The keyword **statistics** is supported only in the NAC unified mode.
user-id *user-id*	Displays information about sessions of a specified user. If this parameter is specified, detailed information about the user is displayed.	The user-id must exist on the device.
detail	Displays detailed information about users.	-
access-type	Displays information about the users using the specified authentication mode.	-

Parameter	Description	Value
admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**]	Displays information about the administrators using the specified authentication mode. • **ftp**: FTP user • **ssh**: SSH user • **telnet**: Telnet user • **terminal**: Terminal user • **web**: Web user	-
wired	Displays information about wired users.	-
wireless	Displays information about wireless users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays information about user sessions on the device.

Precautions

Administrators with low privilege levels cannot view information about administrators with high privilege levels.

If the character string of the user name contains spaces (for example, a b), you can run the **display access-user username "a b"** command to view online users.

If the character string of the user name contains spaces and quotation marks ("") simultaneously, you cannot use the user name to view online users. In this case, you can run the **display access-user | include** *username* command to view the user ID of the online user, and then run the **display access-user user-id** *user-id* command to view the user. Alternatively, you can run the **cut access-user user-id** *user-id* command to disconnect the user.

When displaying VPN user entries based on user IP address, you must set the **vpn-instance** *vpn-instance-name* parameter to specify the VPN instance to which the IP address belongs.

If **user-id** is specified, detailed information about the specified user is displayed. If **user-id** is not specified, brief information about all online users is displayed, including the user ID, user name, IP address, and MAC address of each user.

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

When you run the **display access-user** command without specifying any parameter to view user information and the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following the 19th character; that is, only 22 characters are displayed. When you run the **display access-user** command with parameters specified to view detailed information about the user table, all the characters of **username** are displayed, and the rule for converting special characters remains unchanged.

When **interface** is specified, the device displays the connection information of online wired users on the interface.

When querying user information based on interfaces, MAC addresses, or VLANs, the device only displays information about 802.1X, Portal, or MAC address authentication users.

Example

Display information about user sessions on the device.

```
<HUAWEI> display access-user
  ------------------------------------------------------------------------------------------------
  UserID Username                  IP address                MAC           Status
  ------------------------------------------------------------------------------------------------
  1      normal@local              -                         xxxx-xxxx-xxxx    Success
  62     005500000001                192.168.1.121           xxxx-xxxx-xxx1    Open
  32675  fztest                    -                       xxxx-xxxx-xxx2    Success
  16019  b002404                   192.168.1.2             xxxx-xxxx-xxx3    Success
  ------------------------------------------------------------------------------------------------
 Total: 4, printed: 4
```

NOTE

If you specify the **include** or **exclude** parameter in the command, the values of **Total** and **printed** are still the total number of users.

Display information about the user with the user ID 1.

```
<HUAWEI> display access-user user-id 1
Basic:
  User ID                   : 1
  User name                   : normal
  Domain-name                   : rds
  User MAC                  : xxxx-xxxx-xxxx
  User IP address             : 10.124.1.253
  User vpn-instance             : -
  User IPv6 address             : -
  User access Interface         : GigabitEthernet0/0/1
  User vlan event             : Success
  QinQVlan/UserVlan             : 0/20
  User vlan source            : user request
  User access time            : 2014/03/31 15:38:55
```



```
  User accounting session ID      : esap_lm000000000001245****8016032
  Option82 information            : -
  User access type                : MAC
  HTTP User_Agent                 : Mozilla/4.0 (compatible; MSIE 7.0; Windows N
                                  T 5.1; Trident/4.0; aff-kingsoft-ciba; .NET4
                                  .0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR
                                  3.0.4506.2152; .NET CLR 3.5.30729)
  DHCP option ID                  : 12
  DHCP option content             : [ASCII]
  DHCP option ID                  : 55
  DHCP option content             : [HEX]010F03062C2E2F
  DHCP option ID                  : 60
  DHCP option content             : [ASCII]MSFT 5.0
  User Privilege                  : 15
  Terminal Device Type            : Data Terminal
  Dynamic ACL ID(Effective)       : 3100
  Dynamic group index(Effective)  : 10
  Dynamic group name(Effective)   : group10
  Session Timeout                 : 1800(s) (local), Remaining: 1740(s)
  Termination Action              : RE-AUTHENTICATION

AAA:
  User authentication type        : MAC authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : RADIUS
```

Display the user with the user ID 62.

```
<HUAWEI> display access-user user-id 62
Basic:
  User ID                         : 62
  User name                       : test
  Domain-name                     : -
  User MAC                        : xxxx-xxxx-xxxx
  User IP address                 : 192.168.1.121
  User vpn-instance               : -
  User IPv6 address               : -
  User access Interface           : Wlan-Dbss3:152
  User vlan event                 : Open
  QinQVlan/UserVlan               : 0/125
  User vlan source                : user request
  User access time                : 2015/07/10 11:27:12
  User accounting session ID      : esap_lm000000000001245****8016032
  Option82 information            : -
  User access type                : None
  HTTP User_Agent                 : Mozilla/4.0 (compatible; MSIE 7.0; Windows N
                                  T 5.1; Trident/4.0; aff-kingsoft-ciba; .NET4
                                  .0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR
                                  3.0.4506.2152; .NET CLR 3.5.30729)
  DHCP option ID                  : 12
  DHCP option content             : [ASCII]
  DHCP option ID                  : 55
  DHCP option content             : [HEX]010F03062C2E2F
  DHCP option ID                  : 60
  DHCP option content             : [ASCII]MSFT 5.0
  Redirect ACL ID(Effective)      : 3001
  User Privilege                  : 15
  AP ID                           : 152
  AP name                         : ap-152
  Radio ID                        : 0
  AP MAC                          : 00e0-fc76-e360
  SSID                            : 57-open
  Online time                     : 23(s)
  iConnect info                   : https://example.com:1000/XXXX

AAA:
  User authentication type        : None
  Current authentication method   : None
```



```
  Current authorization method    : Local
  Current accounting method       : None
```

Display the user with the user ID 32675.

```
<HUAWEI> display access-user user-id 32675
Basic:
  User ID                     : 32675
  User name                   : fztest
  Domain-name                 : fz
  User MAC                    : xxxx-xxxx-xxxx
  User IP address             : -
  User IPv6 address           : -
  User access Interface       : Eth-Trunk1
  User vlan event             : Success
  QinQVlan/UserVlan           : 0/18
  User vlan source            : user request
  User access time            : 2015/02/11 21:51:58
  User accounting session ID  : esap_lm000000000001245****8016032
  Option82 information        : -
  User access type            : 802.1x
  Redirect ACL ID(Effective)  : 3001
  User Privilege              : 15
  AS ID                       : 1
  AS name                     : test
  AS IP                       : 192.168.1.11
  AS MAC                      : 00e0-fc76-ee60
  AS Interface                : GigabitEthernet0/0/1
  Terminal Device Type        : Data Terminal

AAA:
  User authentication type    : 802.1x authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : RADIUS
```

Display the user with the user ID 16019.

```
<HUAWEI> display access-user user-id 16019
Basic:
  User ID                     : 16019
  User name                   : b002404
  Domain-name                 : abc
  User MAC                    : xxxx-xxxx-xxxx
  User IP address             : 192.168.1.2
  User vpn-instance           : -
  User IPv6 address           : FC00:3::5689:98FF:FE01:583D
  User IPv6 link local address    : FE80::5689:98FF:FE01:583D
  User access Interface       : GigabitEthernet0/0/1
  User vlan event             : Success
  QinQVlan/UserVlan           : 20/21
  User vlan source            : user request
  User access time            : 2016/08/16 18:32:16
  User accounting session ID  : HUAWEI000000000001245****8016032
  Option82 information        : -
  User PIR(Kbps)              : 5000
  User flow mapping name      : zt
  User flow queue name        : zt
  User access type            : MAC
  Redirect ACL ID(Effective)  : 3001
  Terminal Device Type        : Data Terminal
  User inbound data flow(Packet)  : -
  User inbound data flow(Byte)    : -
  User outbound data flow(Packet) : -
  User outbound data flow(Byte)   : -
  User Lease                  : 600(s)
  ISP   VLAN                  : 1000
  ISP Interface               : GigabitEthernet60/1/17
AAA:
  User authentication type    : MAC authentication
```



```
Current authentication method   : RADIUS
Current authorization method    : -
Current accounting method       : None
```

NOTE

When an Eth-Trunk contains a card that does not support a specified function, the message "The Eth-Trunk contains a card that does not support this function" is displayed behind the corresponding item.

Table 13-6 Description of the **display access-user** command output

Item	Description
Basic	Basic information about a user.
UserID/User ID	Index of a user.
Username/User name	User name.
Domain-name	User domain.
MAC/User MAC	MAC address of a user.
IP address/User IP address	IP address of a user.
User vpn-instance	User VPN instance.
User IPv6 address	IPv6 address of a user.
User IPv6 link local address	IPv6 link-local address.
User access Interface	Access interface connected to a user.
Status/User vlan event	Whether a user joins a VLAN. • Open: For a wired user, the user goes online through the open function upon authentication failure. For wireless users, no authentication is performed. • Success: authentication is successful • Pre-authen: pre-authentication • Client-no-resp: the client does not respond • Fail-authorized: authorization upon authentication failure • Web-server-down: web server is Down • Aaa-server-down: AAA server is Down

Item	Description
QinQVlan/UserVlan	VLAN that a user belongs to. ● In QinQ applications, QinQVlan indicates the outer VLAN ID and UserVlan indicates the inner VLAN ID. ● For a common VLAN, UserVlan indicates the VLAN ID, and QinQVlan is 0.
User vlan source	Source of a user VLAN. ● server vlan: The VLAN is delivered by the remote server. ● server vlan pool: VLAN pool delivered by the remote server ● user group vlan: the VLAN is bound to a user group. This parameter is available only in common mode. ● user group vlan pool: VLAN pool bound to a user group This parameter is available only in common mode. ● service scheme vlan: The VLAN is configured in the service scheme view. ● local event vlan: The authorized VLAN (guest or survival) is configured locally. ● user request: The VLAN is carried in the user request (authentication request).
User access time	Time when a user goes online. If a time zone is configured and the daylight saving time begins, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST.
User accounting session ID	ID of an accounting session.
Option82 information	Option 82 of a user.
User PIR(Kbps)	Peak Information Rate (PIR) in kbit/s.
User flow mapping name	Name of the user flow mapping template.
User flow queue name	Name of the user flow queue.

Item	Description
User access type	Access type of a user. For the related command, see **local-user service-type**.
Redirect ACL ID(Effective)	User redirect ACL ID: ● Effective: The ACL takes effect. ● Ineffective: The ACL does not take effect. The possible reason is that the ACL is not configured on the device.
User Privilege	Level of a user.
Terminal Device Type	Terminal device type of a user.
HTTP User_Agent	User-Agent information in HTTP packets.
DHCP option ID	Value of a DHCP option.
DHCP option content	Content of a DHCP option. **NOTE** If a DHCP option contains invisible characters, it is displayed in hexadecimal format and starts with [HEX]. Otherwise, it is displayed as a character string and starts with [ASCII].
Dynamic group index(Effective)	ID of a UCL group. This option is available only in NAC unified mode.
Dynamic group name(Effective)	Name of a UCL group. This option is available only in NAC unified mode.
Session Timeout	Timeout interval of sessions. ● *xx*(s) (local): reauthentication interval of a locally configured MAC or 802.1X user. ● *xx*(s) (server): Session-Timeout (27) attribute delivered by the RADIUS server. This attribute indicates the remaining time of the service provided to a user.
Remaining	Remaining session time.
Termination Action	Action taken when a session times out. ● RE-AUTHENTICATION: authentication is performed again ● OFFLINE: the user is disconnected.
AP ID	ID of the AP connected to users.

Item	Description
AP name	Name of the AP connected to users.
Radio ID	ID of the radio.
AP MAC	MAC address of the AP connected to users.
SSID	SSID of a STA.
Online time	STA online time.
iConnect info	Identity information of iConnect terminals.
AAA	AAA information about a user.
User authentication type	Authentication type of a user, which depends on the access type of the user.
Current authentication method	Authentication method used for a user.
Current authorization method	Current authorization method.
Current accounting method	Current accounting method.
AS ID	ID of the access devices in policy association network.
AS name	Name of the access devices in policy association network.
AS IP	IP address of the access devices in policy association network.
AS MAC	MAC address of the access devices in policy association network.
AS Interface	Interface of the access devices in policy association network.
User inbound data flow(Packet)	Data traffic (number of packets) from users to the device.
User inbound data flow(Byte)	Data traffic (number of bytes) from users to the device.
User outbound data flow(Packet)	Data traffic (number of packets) from the device to users.
User outbound data flow(Byte)	Data traffic (number of bytes) from the device to users.
User Lease	User lease.
ISP VLAN	Authorized outbound interface VLAN.
ISP Interface	Authorized outbound interface.

Item	Description
Number of user-group car	Number of users whose rate is limited by the CAR value authorized. If this item is not displayed, there are no such users.
web-server IP address	Portal server IP address. This field is displayed only when the Portal or HACA protocol is used for Portal authentication.
User flow mapping name	Authorized flow mapping profile.
SAC profile name	Authorized SAC profile.
DACL group name	Name of the authorized DACL group. It is delivered by the RADIUS server through the RADIUS attribute 26-82 (HW-Data-Filter). • Effective: The DACL group name has taken effect. • Ineffective. The DACL group name does not take effect.

13.1.41 display access-user user-name-table statistics

Function

The **display access-user user-name-table statistics** command displays statistics on users who access the network after the number of users is limited based on the user name.

Format

display access-user user-name-table statistics { **all** | **username** *username* }

Parameters

Parameter	Description	Value
all	Displays statistics on all users.	-
username *username*	Displays statistics on users with a specified user name.	The value is an existing user name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the number of access users is limited based on the user name using the **access-limit user-name max-num** command, you can run the **display access-user user-name-table statistics** command to check related statistics including the maximum number of access users and IP and MAC addresses of access users.

NOTE

Statistics about pre-connection users are not included in the statistics displayed in this command output.

Example

Display statistics on all users who access the network after the number of access users is limited based on the user name.

```
<HUAWEI> display access-user user-name-table statistics all
------------------------------------------------------------------------------
 Username              Current num       Access limit max num
------------------------------------------------------------------------------
 test@123              8                 8
------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display detailed statistics on users with the user name **test@123** who access the network after the number of access users is limited based on the user name.

```
<HUAWEI> display access-user user-name-table statistics username test@123

Basic Info:
 User name                : test@123
 Current num              : 8
 Access limit max num     : 8
Detail Info:
------------------------------------------------------------------------------
 UserID      Username             IP address      MAC
------------------------------------------------------------------------------
 16016       test@123             192.168.8.139   00e0-fcf1-0794
 16017       test@123             192.168.8.140   00e0-fcf1-0795
 16018       test@123             192.168.8.141   00e0-fcf1-0796
 16019       test@123             192.168.8.142   00e0-fcf1-0797
 16020       test@123             192.168.8.143   00e0-fcf1-0798
 16021       test@123             192.168.8.144   00e0-fcf1-0799
 16022       test@123             192.168.8.145   00e0-fcf1-079a
 16023       test@123             192.168.8.146   00e0-fcf1-079b
------------------------------------------------------------------------------
Total: 8, printed: 8
```


Table 13-7 Description of the **display access-user user-name-table statistics** command output

Item	Description
Basic Info	Basic information.
User name or Username	User name.
Current num	Number of current access users.
Access limit max num	Maximum number of access users.
Detail Info	Detailed information.
UserID	User ID.
IP address	User's IP address.
MAC	User's MAC address.
Total: *m*, printed: *n*	Total number (*m*) of entries and number (*n*) of displayed entries.

13.1.42 display accounting-scheme

Function

The **display accounting-scheme** command displays the configuration of accounting schemes, including accounting scheme names and accounting modes.

Format

display accounting-scheme [*accounting-scheme-name*]

Parameters

Parameter	Description	Value
accounting-scheme-name	Specifies the name of an accounting scheme.	The accounting scheme must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the accounting scheme configuration is complete, run the **display accounting-scheme** command to check whether the accounting scheme configuration is correct.

Before applying an accounting scheme to a domain, run the **display accounting-scheme** command to check whether configuration of the accounting scheme is correct.

Precautions

If the name of an accounting scheme is specified, the **display accounting-scheme** command displays the detailed accounting scheme configuration. Otherwise, this command displays only the summary of accounting schemes.

Example

Display the summary of all accounting schemes.

```
<HUAWEI> display accounting-scheme
  ------------------------------------------------------------------------
  Accounting-scheme-name          Accounting-method        scheme-index
  ------------------------------------------------------------------------
  default                         None                     0
  radius-1                        RADIUS                     1
  tacas-1                         HWTACACS                     3

  ------------------------------------------------------------------------
  Total of accounting-scheme: 3
```

Display the detailed configuration of the default accounting scheme.

```
<HUAWEI> display accounting-scheme default

  Accounting-scheme-name               : default
  Accounting-method                  : None
  Realtime-accounting-switch           : Disabled
  Realtime-accounting-interval(min)    : -
  Start-accounting-fail-policy         : Offline
  Realtime-accounting-fail-policy      : Online
  Realtime-accounting-failure-retries  : 3
```

Table 13-8 Description of the **display accounting-scheme** command output

Item	Description
scheme-index	Scheme index.
Accounting-scheme-name	Name of an accounting scheme. To create an accounting scheme, run the **accounting-scheme (AAA view)** command.

Item	Description
Accounting-method	Accounting mode in the accounting scheme: ● HWTACACS: indicates that an HWTACACS server performs accounting. ● None: indicates that accounting is not performed. ● RADIUS: indicates that a RADIUS server performs accounting. ● HACA: indicates that an HACA server performs accounting. To configure the accounting mode, run the **accounting-mode** command.
Realtime-accounting-switch	Whether the real-time accounting function is enabled: ● Disabled: indicates that the real-time accounting function is disabled. ● Enabled: indicates that the real-time accounting function is enabled. To configure the real-time accounting function, run the **accounting realtime** command.
Realtime-accounting-interval(min)	Real-time accounting interval. To configure the real-time accounting interval, run the **accounting realtime** command.
Start-accounting-fail-policy	Policy used in case of accounting-start failures: ● Offline: indicates that the device disconnects users. ● Online: indicates that the device keeps users online. To configure a policy used in case of accounting-start failures, run the **accounting start-fail** command.

Item	Description
Realtime-accounting-fail-policy	Policy used in case of real-time accounting failures: • Offline: indicates that the device disconnects users. • Online: indicates that the device keeps users online. To configure a policy used in case of real-time accounting failures, run the **accounting interim-fail** command.
Realtime-accounting-failure-retries	Number of retries before a real-time accounting failure is confirmed. To configure the number of retries, run the **accounting interim-fail** command.

13.1.43 display authentication-scheme

Function

The **display authentication-scheme** command displays the configuration of authentication schemes.

Format

display authentication-scheme [*authentication-scheme-name*]

Parameters

Parameter	Description	Value
authentication-scheme-name	Specifies the name of an authentication scheme.	The authentication scheme must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether an authentication scheme is configured correctly, run the **display authentication-scheme** command.

Precautions

If the **display authentication-scheme** command is executed in the authentication scheme view or the name of an authentication scheme is specified in the command, this command displays detailed authentication scheme configuration. Otherwise, this command displays only summary information of authentication schemes.

Example

Display summary information of all authentication schemes.

```
<HUAWEI> display authentication-scheme
  ------------------------------------------------------------------------
 Authentication-scheme-name        Authentication-method     scheme-index
  ------------------------------------------------------------------------
  default                          Local                     0
  radius                           RADIUS                    1
  ------------------------------------------------------------------------
  Total of authentication scheme: 2
```

Display detailed configuration of the authentication scheme named **default**.

```
<HUAWEI> display authentication-scheme default

  Authentication-scheme-name          : default
  Authentication-method               : Local
  Radius authentication-type of admin : PAP(all)
  server no-response accounting       : NO
  server no-response authorization    : NO
  Location after radius reject        : None
```

Table 13-9 Description of the **display authentication-scheme** command output

Item	Description
scheme-index	Scheme index.
Authentication-scheme-name	Name of an authentication scheme. To create an authentication scheme, run the **authentication-scheme (AAA view)** command.
Authentication-method	Authentication mode in an authentication scheme. To configure an authentication mode in an authentication scheme, run the **authentication-mode (authentication scheme view)** command.

Item	Description
Radius authentication-type of admin	Access type of administrators on whom CHAP authentication is performed during RADIUS authentication. The value can be: ● PAP(all): PAP authentication is performed on administrators of all access types when they are authenticated using RADIUS. ● CHAP(ftp) PAP (other): CHAP authentication is performed on FTP users whose access types are displayed in brackets () when they are authenticated using RADIUS, and PAP authentication is performed on the administrators of other access types. To configure the access type, run the **authentication-type radius chap access-type admin** command.
server no-response accounting	Whether the device continues to send accounting packets after local authentication is performed for a user who does not receive any response from the server. The value can be: ● YES: The device continues to send accounting packets. ● NO: The device does not send accounting packets. To configure this function, run the **server no-response accounting** command.
server no-response authorization	Whether the device continues to send authorization packets after local authentication is performed for a user who does not receive any response from the server. The value can be: ● YES: The device continues to send authorization packets. ● NO: The device does not send authorization packets. To configure this function, run the **server no-response authorization** command.

Item	Description
Location after radius reject	Whether a user is authenticated using another authentication mode after the user's RADIUS authentication request is rejected. The value can be: • None: The user is not authenticated using another authentication mode after the user's RADIUS authentication request is rejected and the authentication process ends. • Local: The user is authenticated using the local authentication mode after the user's RADIUS authentication request is rejected. To configure this parameter, run the **radius-reject local** command.

13.1.44 display authorization-scheme

Function

The **display authorization-scheme** command displays the configuration of authorization schemes.

Format

display authorization-scheme [*authorization-scheme-name*]

Parameters

Parameter	Description	Value
authorization-scheme-name	Specifies the name of an authorization scheme.	The authorization scheme must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the authorization scheme configuration is complete, run the **display authorization-scheme** command to check whether the authorization scheme configuration is correct.

Before applying an authorization scheme to a domain, run the **display authorization-scheme** command to check whether the authorization scheme meets requirements.

Precautions

If the name of an authorization scheme is specified, this command displays the detailed configuration of the authorization scheme. Otherwise, this command displays only the summary of authorization schemes.

Example

Display the summary of authorization schemes.

```
<HUAWEI> display authorization-scheme
  ------------------------------------------------------------------------
 Authorization-scheme-name          Authorization-method        scheme-index
  ------------------------------------------------------------------------
  default                        Local                    0
  scheme0                          Local                    1
  ------------------------------------------------------------------------
  Total of authorization-scheme: 2
```

Display the detailed configuration of the authorization scheme **scheme0**.

```
<HUAWEI> display authorization-scheme scheme0
------------------------------------------------------------------------------
 Authorization-scheme-name   : scheme0
 Authorization-method        : Local
 Authorization-cmd level  0   : Disabled
 Authorization-cmd level  1   : Disabled
 Authorization-cmd level  2   : Disabled
 Authorization-cmd level  3   : Disabled
 Authorization-cmd level  4   : Disabled
 Authorization-cmd level  5   : Disabled
 Authorization-cmd level  6   : Disabled
 Authorization-cmd level  7   : Disabled
 Authorization-cmd level  8   : Disabled
 Authorization-cmd level  9   : Disabled
 Authorization-cmd level 10   : Disabled
 Authorization-cmd level 11   : Disabled
 Authorization-cmd level 12   : Disabled
 Authorization-cmd level 13   : Disabled
 Authorization-cmd level 14   : Disabled
 Authorization-cmd level 15   : Disabled
 Authorization-cmd no-response-policy    : Online
------------------------------------------------------------------------------
```

Table 13-10 Description of the **display authorization-scheme** command output

Item	Description
scheme-index	Scheme index.
Authorization-scheme-name	Name of an authorization scheme. To configure this parameter, run the **authorization-scheme (AAA view)** command.

Item	Description
Authorization-method	Authorization mode configured for an authorization scheme. To configure this parameter, run the **authorization-mode** command.
Authorization-cmd level	Whether the command authorization function is enabled for a user with a specified level: • Disabled: The command authorization function is disabled. • Enabled: The command authorization function is enabled. To configure this parameter, run the **authorization-cmd** command.
Authorization-cmd no-response-policy	Policy used when command authorization fails: allows users to go online.

13.1.45 display domain

Function

The **display domain** command displays the domain configuration.

Format

display domain [**name** *domain-name*]

Parameters

Parameter	Description	Value
name *domain-name*	Specifies the domain name. If this parameter is not specified, brief information about all domains is displayed.	The domain name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a domain is created using the **domain** command and is configured, you can run the **display domain** command to view the domain configuration.

Example

Display brief information about all domains.

```
<HUAWEI> display domain
  ------------------------------------------------------------------------------
  index    DomainName
  ------------------------------------------------------------------------------
  0        default
  1        default_admin
  ------------------------------------------------------------------------------
  Total: 2
```

Table 13-11 Description of the **display domain** command output

Item	Description
index	Domain index. To configure this parameter, run the **domain (AAA view)** command.
DomainName	Domain name. To configure this parameter, run the **domain (AAA view)** command.

Display the configuration of the domain **default**.

```
<HUAWEI> display domain name default

  Domain-name                     : default
  Domain-index                    : 0
  Domain-state                    : Active
  Authentication-scheme-name      : default
  Accounting-scheme-name          : default
  Authorization-scheme-name       : -
  Service-scheme-name             : -
  RADIUS-server-template          : -
  Accounting-copy-RADIUS-template : -
  HWTACACS-server-template        : -
  HACA-server-template            : -
  User-group                      : -
  Push-url-address                : -
  Accounting-DualStack-Separate   : -
```

Table 13-12 Description of the **display domain name** command output

Item	Description
Domain-name	Domain name. To configure this parameter, run the **domain (AAA view)** command.

Item	Description
Domain-index	Domain index. To configure this parameter, run the **domain (AAA view)** command.
Domain-state	Domain status. • Active: indicates that the domain is activated. • Block: indicates that the domain is blocked. To configure this parameter, run the **state (AAA domain view)** command.
Authentication-scheme-name	Name of the authentication scheme used in a domain. To configure this parameter, run the **authentication-scheme (AAA domain view)** command.
Accounting-scheme-name	Name of the accounting scheme used in a domain. To configure this parameter, run the **accounting-scheme (AAA domain view)** command.
Authorization-scheme-name	Name of the authorization scheme used in a domain. To configure this parameter, run the **authorization-scheme (AAA domain view)** command.
Service-scheme-name	Name of the service scheme used in a domain. To configure this parameter, run the **service-scheme (AAA domain view)** command.
RADIUS-server-template	Name of the RADIUS server template used in a domain. To configure this parameter, run the **radius-server (AAA domain view)** command.
Accounting-copy-RADIUS-template	RADIUS server template for level-2 accounting used in a domain. To configure this parameter, run the **accounting-copy radius-server** command.
HWTACACS-server-template	Name of the HWTACACS server template used in a domain. To configure this parameter, run the **hwtacacs-server** command.
HACA-server-template	Name of the HACA server template used in a domain.
User-group	Name of the user group for users in a domain. To configure this parameter, run the **user-group (AAA domain view)** command.

Item	Description
Push-url-address	Pushed URL used in a domain. To configure this parameter, run the **force-push** command.
Accounting-DualStack-Separate	Whether separate statistics collection or separate rate limiting of IPv4 and IPv6 traffic is enabled: ● enable: The function is enabled. ● -: The function is disabled. To configure this parameter, run the **accounting dual-stack separate** command.

13.1.46 display local-user

Function

The **display local-user** command displays information about local users.

Format

display local-user [**domain** *domain-name* | **state** { **active** | **block** } | **username** *user-name*] *

Parameters

Parameter	Description	Value
domain *domain-name*	Displays information about local users in a specified domain.	The domain name must already exist.
state { **active**	**block** }	Displays the attributes of local users in the specified state. ● **active**: indicates the active state. ● **block**: indicates the blocking state.	-
username *user-name*	Displays information about a specified local user name.	The user name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **display local-user** command output helps you check the configuration of local users and isolate faults related to the local users.

Precautions

If no parameter is specified, brief information about all local users is displayed. If a parameter is specified, detailed information about the specified local user is displayed.

Low-level users cannot view information about high-level users.

Example

Display brief information about local users.

```
<HUAWEI> display local-user
 ------------------------------------------------------------------------------
 User-name                      State  AuthMask  AdminLevel
 ------------------------------------------------------------------------------
 user-a                         A      A         0
 user-c                         A      A         0
 ------------------------------------------------------------------------------
 Total 2 user(s)
```

Display detailed information about the local user **user-a**.

```
<HUAWEI> display local-user username user-a
 The contents of local user(s):
 Password            : ***************
 State               : active
 Service-type-mask   : A
 Privilege level     : -
 Ftp-directory       : -   HTTP-directory      : -
 Access-limit        : Yes
 Access-limit-max    : 4294967295
 Accessed-num        : 0
 Idle-timeout        : -
 User-group          : -
 Original-password   : No
 Password-set-time   : 2019-12-01 18:42:57+01:00 DST
 Password-expired    : No
 Password-expire-time : -
 Account-expire-time  : -
 Last login ip       : 192.168.240.235
 Last login time     : 2019-03-21 09:38:24+08:00
 Login fail count    : 0
 Password expire in  : -
 Ftp-privilege       : write
```


NOTE

For a local user who fails to log in to the device but is not locked, **Retry-time-left** is displayed. For a local user whose initial password is changed, **Change password retry-count-left** is displayed. When the number of continuous login failures or the number of initial password change failures reaches the limit specified using the **local-aaa-user wrong-password** command, the user is locked.

When the number of user login failures or the number of initial password change failures does not reach the limit specified using the **local-aaa-user wrong-password** command, the user is not locked. If the limit is changed using the **local-aaa-user wrong-password** command, and the new limit is smaller than the number of user login failures or the number of initial password change failures, the user still has a change to try to log in to the device or change the password. In this case, **Retry-time-left** or **Change password retry-count-left** is displayed as 1.

Display information about local user **user1** who fails to log in to the device.

```
<HUAWEI> display local-user username
user1
  The contents of local user(s):
  Password            : ****************
  State               : active
  Service-type-mask    : T
  Privilege level      : 0
  Ftp-directory        : -
  HTTP-directory       : -
  Access-limit         : -
  Accessed-num         : 0
  Idle-timeout         : -
  Retry-interval       : 4 Min(s)
  Retry-time-left      : 1
  Original-password    : Yes
  Password-set-time    : 2019-01-27 13:26:55+08:00
  Password-expired     : No
  Password-expire-time : -
  Account-expire-time  : -
  Password expire in   : -
  Ftp-privilege        : write
```

Display information about local user **user1** whose initial password fails to be changed.

```
<HUAWEI> display local-user username user1
  The contents of local user(s):
  Password            : ****************
  State               : active
  Service-type-mask    : T
  Privilege level      : 0
  Ftp-directory        : -
  HTTP-directory       : -
  Access-limit         : -
  Accessed-num         : 1
  Idle-timeout         : -
  Change password retry-interval  : 4 Min(s)
  Change password retry-count-left: 3
  Original-password    : Yes
  Password-set-time    : 2019-01-27 13:26:55+08:00
  Password-expired     : No
  Password-expire-time : -
  Account-expire-time  : -
  Password expire in   : -
  Ftp-privilege        : write
```

Display information about local users in blocking state.

```
<HUAWEI> display local-user state block
  ------------------------------------------------------------------------------
  User-name                 State  AuthMask  AdminLevel
BlockTime
  ------------------------------------------------------------------------------
  test2                     B      T         0          2018-04-10 01:55:11-00:00
```



```
--------------------------------------------------------------------------------
Total 1 user(s)
```

Display information about local user **test2** in blocking state.

```
<HUAWEI> display local-user state block username test2
 The contents of local user(s):
 Password            : **********
 State               : block
 Service-type-mask   : T
 Privilege level     : 0
 Ftp-directory       : -
 HTTP-directory      : -
 Access-limit        : -
 Accessed-num        : 0
 Idle-timeout        : -
 Block-time-left     : 8 Min(s)
 Original-password   : Yes
 Password-set-time   : 2019-01-27 13:26:55+08:00
 Password-expired    : No
 Password-expire-time : -
 Account-expire-time  : -
 Password expire in   : -
 Ftp-privilege       : write
```

Table 13-13 Description of the **display local-user** command output

Item	Description
User-name	Name of the local user. To configure this parameter, run the **local-user** command.
State	State of the local user: ● A: Active ● B: Block To configure this parameter, run the **local-user** command.

Item	Description
AuthMask	Access type of the local user. • T: indicates the Telnet users. • M: indicates the terminal users, which usually refer to the console users. • S: indicates the SSH users. • F: indicates the FTP users. • W: indicates the web users. • X: indicates the 802.1X users. • A: indicates all access types. • H: indicates the HTTP users. • D: indicates the X25-PAD users. • P: indicates the PPP users. • Combination: For example, MH indicates either a terminal user or an HTTP user. • I: indicates the API user, which is typically used for NETCONF access. To configure this parameter, run the **local-user service-type** command.
AdminLevel	Local user level. To configure this parameter, run the **local-user** command.
Password	Password of the local user. To configure this parameter, run the **local-user** command.
Service-type-mask	Service type of the local user. Same as the AuthMask type. To configure this parameter, run the **local-user service-type** command.
Privilege level	Local user level. To configure this parameter, run the **local-user** command.
Ftp-directory	FTP directory of the local user. To configure this parameter, run the **local-user** command.
Ftp-privilege	The Permission to operate the FTP directory of the local user. To configure this parameter, run the **local-user username ftp-privilege** command.

Item	Description
HTTP-directory	HTTP directory of the local user. To configure this parameter, run the **local-user** command.
Access-limit	Whether the maximum number of sessions of the local user is configured. To configure this parameter, run the **local-user** command.
Access-limit-max	Maximum number of sessions of the local user. To configure this parameter, run the **local-user** command.
Accessed-num	Number of established sessions.
Idle-timeout	Idle timeout interval. To configure this parameter, run the **local-user** command.
User-group	Authorization information of the user group to which the local user is bound. To configure this parameter, run the **local-user** command.
Original-password	Whether the password of a local user is the initial password: ● Yes ● No To configure this parameter, run the **password alert original** command.
Password-set-time	Time when the local user's password is created. The value is in format local time + DST offset.
Password-expired	Whether a local user's password has expired: ● Yes ● No
Password-expire-time	Time when the local user's password expires. The value is in format local time + DST offset. To configure this parameter, run the **password expire** command.
Account-expire-time	Expiry time of a local user account. The value is in format local time + DST offset. To configure this parameter, run the **local-user expire-date** command.
Last login ip	IP address for user login. This item can be displayed only for administrators.

Item	Description
Last login time	User login time. This item can be displayed only for administrators.
Login fail count	Number of user login failures. This item can be displayed only for administrators.
Password expire in	Validity period of the password for a local user to log in to the device.
BlockTime/Block-time-left	Remaining time of locked local users. (Local users are locked because the entered password is incorrect consecutively.)
Retry-interval	Login retry interval before a local user is locked. To configure this parameter, run the **local-aaa-user wrong-password** command.
Retry-time-left	Remaining number of login retries before a local user is locked. To configure this parameter, run the **local-aaa-user wrong-password** command.
Change password retry-interval	Retry interval for changing the initial password of a local user before the user is locked. To configure this parameter, run the **local-aaa-user wrong-password** command.
Change password retry-count-left	Remaining number of initial password change retries before a local user is locked. To configure this parameter, run the **local-aaa-user wrong-password** command.

13.1.47 display local-user expire-time

Function

The **display local-user expire-time** command displays the time when local accounts expire.

Format

display local-user expire-time

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The command output helps you diagnose and rectify the faults related to local user passwords.

Example

Display the time when local accounts expire.

```
<HUAWEI> display local-user expire-time
--------------------------------------------------------------------------------
Username              Password-expire      Account-expire          Expired
--------------------------------------------------------------------------------
zsh                2014-12-01 21:25:44   -                    NO
mm001                2014-12-01 21:29:58   -                      NO
--------------------------------------------------------------------------------
Total: 2, printed: 2
```

Table 13-14 Description of the **display local-user expire-time** command output

Item	Description
Username	Local account name. To configure this parameter, run the **local-user** command.
Password-expire	Number of days after which the password expires. To configure this parameter, run the **password expire** command.
Account-expire	Account expiration time. To configure this parameter, run the **local-user expire-date** command.
Expired	Whether the local account has expired: ● YES ● NO **NOTE** The displayed value and actual value may have a difference within one minute; there is a possibility that the password has expired, but the displayed value is **NO**. When the local user account or password has expired, the local user becomes invalid.

13.1.48 display local-aaa-user password policy

Function

The **display local-aaa-user password policy** command displays the password policy of local user.

Format

display local-aaa-user password policy { **access-user** | **administrator** }

Parameters

Parameter	Description	Value
access-user	Indicates the password policy of local access users.	-
administrator	Indicates the password policy of local administrator.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After configuring the password policy for local users, you can run the **display local-aaa-user password policy** command to check whether the configuration is correct.

Example

Display the password policy of local access users.

```
<HUAWEI> display local-aaa-user password policy access-user
  Password control              : Enable
  Password history              : Enable (history records:5)
```

Table 13-15 Description of the **display local-aaa-user password policy access-user** command output

Item	Description
Password control	Whether the password control function is enabled: • Enable • Disable To configure this function, run the **local-aaa-user password policy access-user** command.

Item	Description
Password history	Whether the historical password recording function is enabled and the maximum number of historical passwords of each user. To configure this function, run the **password history record number** command.

Display the password policy of local administrator.

```
<HUAWEI> display local-aaa-user password policy administrator
  Password control                : Enable
  Password expiration              : Enable (180 days)
  Password history                : Enable (history records:5)
  Password alert before expiration : 30 days
  Password alert original          : Enable
```

Table 13-16 Description of the **display local-aaa-user password policy administrator** command output

Item	Description
Password control	Whether the password control function is enabled: ● Enable ● Disable To configure this function, run the **local-aaa-user password policy administrator** command.
Password expiration	Whether the password expiration function is enabled and password expiration time. To configure this function, run the **password expire** command.
Password history	Whether the historical password recording function is enabled and the maximum number of historical passwords of each user. To configure this function, run the **password history record number** command.
Password alert before expiration	Password expiration prompt days. To configure this function, run the **password alert before-expire** command.
Password alert original	Whether the device prompt users to change the initial passwords: ● Enable ● Disable To configure this function, run the **password alert original** command.

13.1.49 display recording-scheme

Function

The **display recording-scheme** command displays the configuration of recording schemes.

Format

display recording-scheme [*recording-scheme-name*]

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display recording-scheme** command displays the configuration of recording schemes.

Example

Display the configuration of the recording scheme **scheme0**.

```
<HUAWEI> display recording-scheme scheme0
------------------------------------------------------------------
 Recording-scheme-name          : scheme0
 HWTACACS-template-name         : tacas-1
------------------------------------------------------------------
```

Table 13-17 Description of the **display recording-scheme** command output

Item	Description
Recording-scheme-name	Name of the recording scheme. To create a recording scheme, run the **recording-scheme** command.

Item	Description
HWTACACS-template-name	Name of the HWTACACS server template associated with the recording scheme. To associate an HWTACACS server template with a recording scheme, run the **recording-mode hwtacacs** command.

13.1.50 display remote-user authen-fail

Function

The **display remote-user authen-fail** command displays the accounts that fail in remote AAA authentication.

Format

display remote-user authen-fail [**blocked** | **username** *username*]

Parameters

Parameter	Description	Value
blocked	Displays all the remote AAA authentication accounts that have been locked.	-
username *username*	Displays details about the accounts that fail in remote AAA authentication. If the *username* parameter is not specified, basic information about all accounts that fail in remote AAA authentication is displayed.	It is a string of 1 to 253 case-insensitive characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the account locking function is enabled for the users who fail in AAA remote authentication, the device records all failed accounts, including:

- The accounts that failed in authentication and are locked, for example, when the user entered the wrong account name or password too many times.
- The accounts that failed in authentication, but are not locked, for example, when the number of times the account name or password was entered incorrectly did not exceed the limit.

Prerequisites

The **access-user remote authen-fail** command has been executed to enable the account locking function for access users who fail remote authentication. Alternatively, the **administrator remote authen-fail** command has been executed to enable the account locking function for administrators who fail remote authentication.

Precautions

The device cannot back up a recorded account that fails the AAA authentication. If an active/standby switchover policy has been configured on the device, all user entries are cleared when the device completes an active/standby switchover.

Example

Display all accounts that have failed in remote AAA authentication.

```
<HUAWEI> display remote-user authen-fail
  Interval: Retry Interval(Mins)
  TimeLeft: Retry Time Left
  BlockDuration: Block Duration(Mins)
  ------------------------------------------------------------------------------
  Username                Interval  TimeLeft  BlockDuration  UserType
  ------------------------------------------------------------------------------
  www@test                 0         0         65414          administrator
  ------------------------------------------------------------------------------
  Total 1, 1 printed
```

Display all locked accounts.

```
<HUAWEI> display remote-user authen-fail blocked
Interval: Retry Interval(Mins)
TimeLeft: Retry Time Left
BlockDuration: Block Duration(Mins)
-------------------------------------------------------------------------------------------------
Username                Interval  TimeLeft  BlockDuration  BlockTime                UserType
-------------------------------------------------------------------------------------------------
www@test                 0         0         65414          2018-04-23 17:22:09+08:00 administrator
-------------------------------------------------------------------------------------------------
Total 1, 1 printed
```

Display details about the account **test** that failed in remote AAA authentication.

```
<HUAWEI> display remote-user authen-fail username test
  The contents of the user:
  User-type            : Administrator
  Retry interval(Mins)  : 29
  Retry time left       : 4
  Block time left(Mins) : 0
  User state           : Block
```


Table 13-18 Description of the **display remote-user authen-fail** command output

Item	Description
Username	User name.
Interval or Retry interval(Mins)	Authentication retry interval, in minutes. To configure this parameter, run the **access-user remote authen-fail** or **administrator remote authen-fail** command.
TimeLeft or Retry Time Left	Remaining number of consecutive authentication failures. To configure this parameter, run the **access-user remote authen-fail** or **administrator remote authen-fail** command.
BlockDuration or Block time left(Mins)	User account locking duration, in minutes. To configure this parameter, run the **access-user remote authen-fail** or **administrator remote authen-fail** command.
UserType	User type: • administrator • access-user
BlockTime	User account locking time.
Block-time-left	Remaining locking time of an account.
User-state	User status: • Block • Active

13.1.51 display security weak-password-dictionary

Function

The **display security weak-password-dictionary** command displays information about weak passwords on the device.

Format

display security weak-password-dictionary

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a weak password dictionary is loaded to the device, you can run this command to view information about weak passwords on the device.

Example

Display information about the weak password dictionary on the device.

```
<HUAWEI> display security weak-password-dictionary
-------------------------------------------------------------------------------
 Weak Password
-------------------------------------------------------------------------------
 test1
 test2
 test3
-------------------------------------------------------------------------------
 Total: 3
```

Table 13-19 Description of the **display security weak-password-dictionary** command output

Item	Description
Weak Password	Weak password.

13.1.52 display service-scheme

Function

The **display service-scheme** command displays the configuration of service schemes.

Format

display service-scheme [**name** *name*]

Parameters

Parameter	Description	Value
name *name*	Specifies the name of a service scheme.	The service scheme must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display service-scheme** command displays the configuration of service schemes.

Before applying a service scheme to a domain, run the **display service-scheme** command to check whether the service scheme is correct.

Precautions

The **display service-scheme** command displays the detailed configuration if the command is executed in the service scheme view or the name of a service scheme is specified. Otherwise, this command displays only the summary of service schemes.

Example

Display information about all service schemes.

```
<HUAWEI> display service-scheme
  ------------------------------------------------------------------------
  service-scheme-name                   scheme-index
  ------------------------------------------------------------------------
  svcscheme1                            0
  svcscheme2                            1
  ------------------------------------------------------------------------
  Total of service scheme: 2
```

Display the configuration of the service scheme **svcscheme1**.

```
<HUAWEI> display service-scheme name svcscheme1

  service-scheme-name           : svcscheme1
  service-scheme-primary-dns    : -
  service-scheme-secondary-dns  : -
  service-scheme-adminlevel     : 15
  service-scheme-uclgroup-ID    : 10
  service-scheme-uclgroup-name  : u1
  service-scheme-acl-id         : 3001
  service-scheme-ipv6-acl-id    : 3001
  service-scheme-redirect-acl-id: 3001
  service-scheme-vlan           : 10
  service-scheme-priority       : 0
  service-scheme-voicevlan      : enable
  access-limit-username-maxnum  : 10
  service-scheme-qosprofile     : -
  service-scheme-sacprofile     : -
  service-scheme-idlecut-time   : 10
  service-scheme-idlecut-flow   : 20
  service-scheme-idlecut-direct : Inbound and Outbound
```


Table 13-20 Description of the **display service-scheme** command output

Item	Description
service-scheme-name	Name of a service scheme. To create a service scheme, run the **service-scheme (AAA view)** command.
scheme-index	Index of a service scheme.
service-scheme-primary-dns	Address of the primary DNS server. To configure this item, run the **dns** command.
service-scheme-secondary-dns	Address of the secondary DNS server. To configure this item, run the **dns** command.
service-scheme-adminlevel	Level of an administrator. To configure this item, run the **admin-user privilege level** command.
service-scheme-uclgroup-ID	Index of the bound UCL group. To configure this item, run the **ucl-group** command.
service-scheme-uclgroup-name	Name of the bound UCL group. To configure this item, run the **ucl-group** command.
service-scheme-acl-id	Bound ACL number. To configure this item, run the **acl-id** command.
service-scheme-ipv6-acl-id	Bound IPv6 ACL number. To configure this item, run the **acl-id** command.
service-scheme-redirect-acl-id	Number of the ACL used for redirection in the service scheme. To configure this item, run the **redirect-acl** command.
service-scheme-vlan	User VLAN ID. To configure this item, run the **user-vlan** command.
service-scheme-priority	User priority in the service scheme. To configure this item, run the **priority** command.
service-scheme-voicevlan	Whether voice VLAN is enabled. To configure this item, run the **voice-vlan** command.
access-limit-username-maxnum	Maximum number of users who are allowed to access the network using the same user name. To configure this item, run the **access-limit user-name max-num** command.

Item	Description
service-scheme-qosprofile	Name of the bound QoS profile. To configure this item, run the **qos-profile** command.
service-scheme-sacprofile	Name of the bound SAC profile. To configure this item, run the **sac-profile (service scheme view)** command.
service-scheme-idlecut-time	Idle-cut timeout interval, in minutes. To configure this item, run the **idle-cut** command.
service-scheme-idlecut-flow	Threshold for idle-cut traffic, in Kbytes. To configure this item, run the **idle-cut** command.
service-scheme-idlecut-direct	Direction in which idle-cut takes effect for traffic: • Inbound: Idle-cut takes effect for uplink traffic. • Outbound: Idle-cut takes effect for downlink traffic. • Inbound and Outbound: Idle-cut takes effect for uplink and downlink traffic. To configure this item, run the **idle-cut** command.

13.1.53 display vlan pool

Function

The **display vlan pool** command displays configuration of VLAN pools.

Format

display vlan pool { **name** *pool-name* | **all** [**verbose**] }

Parameters

Parameter	Description	Value
name *pool-name*	Displays configuration of a specified VLAN pool.	The VLAN pool must exist.
all [**verbose**]	Displays configuration of all VLAN pools. List of VLANs in the VLAN pool will be displayed if **verbose** is specified.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration of VLAN pools, which facilitates VLAN pool management and maintenance.

Example

Display brief configuration of all VLAN pools.

```
<HUAWEI> display vlan pool all
--------------------------------------------------------------------------------
Name                    Assignment              VLAN total
--------------------------------------------------------------------------------
name                    hash                    0
test                    hash                    128
marketing               hash                    2
--------------------------------------------------------------------------------
Total: 3
```

Table 13-21 Description of the **display vlan pool all** command output

Item	Description
Name	Name of a VLAN pool. To configure the parameter, run the **vlan pool** command.
Assignment	VLAN assignment algorithm in a VLAN pool: ● even: The VLAN assignment algorithm is **even**. ● hash: The VLAN assignment algorithm is **hash**. To configure the parameter, run the **assignment** command.
VLAN total	Number of VLANs in the VLAN pool.
Total	Total number of VLAN pools.

Display configuration of the VLAN pool **test**.

```
<HUAWEI> display vlan pool name test
--------------------------------------------------------------------------------
Name                  : test
Total                 : 21
Assignment            : hash
VLAN Block Time(min)  : 10
Threshold Notify Count: 5
VLAN ID               : 10 to 30
Blocked VLAN ID       : -
--------------------------------------------------------------------------------
```


Table 13-22 Description of the **display vlan pool name** *pool-name* command output

Item	Description
Name	Name of the VLAN pool. To configure the parameter, run the **vlan pool** command.
Total	Number of VLANs in the VLAN pool.
Assignment	VLAN assignment algorithm in a VLAN pool: ● even: The VLAN assignment algorithm is **even**. ● hash: The VLAN assignment algorithm is **hash**. To configure the parameter, run the **assignment** command.
VLAN Block Time(min)	Lockout time of VLANs, in minutes. To configure the parameter, run the **vlan block-time** command. If the default lockout time is used, this field is not displayed.
Threshold Notify Count	Number of times the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN. To configure the parameter, run the **dhcp update vlan assignment threshold** command. If the default parameter value is used, this field is not displayed.
VLAN ID	List of VLANs in the VLAN pool. To configure the parameter, run the **vlan (VLAN pool view)** command.
Blocked VLAN ID	List of VLANs that are locked. After the **dhcp update vlan assignment** command is run, a VLAN is locked and cannot be assigned to users within the specified lockout time if all IP addresses in the VLAN have been assigned. **NOTE** This field takes effect only for wired users. To check the VLAN list of wireless users, run the **display vlan pool name status** command.

13.1.54 dhcp update vlan assignment

Function

The **dhcp update vlan assignment** command enables the function of reassigning VLANs in a VLAN pool.

The **undo dhcp update vlan assignment** command disables the function of reassigning VLANs in a VLAN pool.

By default, the function of reassigning VLANs in a VLAN pool is disabled.

Format

dhcp update vlan assignment

undo dhcp update vlan assignment

Parameters

None

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the VLAN assignment algorithm is **hash**, the VLAN pool assigns VLANs to users based on the hash results of the users' MAC addresses. If the hash results of multiple MAC addresses are the same, available IP addresses in a specific VLAN may be insufficient. To solve this problem, run the **dhcp update vlan assignment** command to lock the VLAN in which all IP addresses have been assigned for a period of time so that the device selects another VLAN from the VLAN pool to assign IP addresses.

Prerequisites

The VLAN assignment algorithm has been set to **hash** using the **assignment hash** command.

Precautions

Before configuring this function, enable DHCP snooping on the interface through which users go online.

This function takes effect only for wired users.

Authentication access devices in the policy association scenario do not support this function.

After the **assignment even** command is run, the **assignment hash** command configuration will be cleared. Exercise caution when running the **assignment even** command.

The locked VLAN will be unlocked in advance if any of the following operations is performed:

- Run the **assignment even** command in the VLAN pool view to set the VLAN assignment algorithm to **even**.
- Run the **undo vlan** command in the VLAN pool view to delete the VLAN from the VLAN pool.
- Run the **undo dhcp update vlan assignment** command in the VLAN pool view to disable the function of reassigning VLANs in the VLAN pool.

Example

Enable the function of reassigning VLANs in a VLAN pool.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] assignment hash
[HUAWEI-vlan-pool-test] dhcp update vlan assignment
```

13.1.55 dhcp update vlan assignment interval

Function

The **dhcp update vlan assignment interval** command sets the interval at which the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN.

The **undo dhcp update vlan assignment interval** command restores the default value.

By default, if the number of times that the VLAN pool module receives the notification from the DHCP module within 3 minutes reaches the value specified using the **dhcp update vlan assignment threshold** command, the VLAN is locked.

NOTE

This command is supported only on the This feature is supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Format

dhcp update vlan assignment interval *interval-value*

undo dhcp update vlan assignment interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval at which the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN.	The value is an integer in the range of 0 to 1440, in minutes. The default value is 3. If the parameter value is set to 0, the VLAN locking function does not take effect.

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the VLAN assignment algorithm is **hash**, the VLAN pool assigns VLANs to users based on the hash results of the users' MAC addresses. If the function of reassigning VLANs in the VLAN pool is enabled on the device, the DHCP module notifies the VLAN pool module that a user fails to obtain an IP address from the IP address pool for a specific VLAN when the user cannot obtain an IP address from the address pool.

To set the interval at which the VLAN pool module receives such a notification, run the **dhcp update vlan assignment interval** command. When the VLAN pool module receives the notification from the DHCP module for the number of times specified using the **dhcp update vlan assignment threshold** command within the specified period, the corresponding VLAN is locked for a period of time. The device then re-authorizes an available VLAN in the VLAN pool to the user. If all VLANs in the VLAN pool are locked, the device authorizes the user with the default VLAN for the interface through which the user goes online.

Precautions

This function takes effect only for wireless users.

Authentication access devices in the policy association scenario do not support this function.

Example

Configure the device to lock a VLAN after the VLAN pool module receives a notification from the DHCP module three times within 5 minutes, indicating that wireless users fail to obtain IP addresses from the IP address pool for the VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] dhcp update vlan assignment threshold 3
[HUAWEI-vlan-pool-test] dhcp update vlan assignment interval 5
```

13.1.56 dhcp update vlan assignment threshold

Function

The **dhcp update vlan assignment threshold** command sets the number of times the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN.

The **undo dhcp update vlan assignment threshold** command restores the default value.

By default, when the VLAN pool module receives a notification from the DHCP module three times, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN, the VLAN is locked.

Format

dhcp update vlan assignment threshold *count*

undo dhcp update vlan assignment threshold

Parameters

Parameter	Description	Value
count	Specifies the number of times that the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN.	The value is an integer in the range of 1 to 255. The recommended value is 3.

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the VLAN assignment algorithm is **hash**, the VLAN pool assigns VLANs to users based on the hash results of the users' MAC addresses. If the function of reassigning VLANs in the VLAN pool is enabled on the device, the DHCP module notifies the VLAN pool module that a user fails to obtain an IP address from the IP address pool for a specific VLAN when the user cannot obtain an IP address from the address pool.

To set the number of times the VLAN pool module receives such a notification from the DHCP module, run the **dhcp update vlan assignment threshold** command. When the number of times that the VLAN pool module receives the notification from the DHCP module reaches the configured value, the VLAN is locked for a certain period. The device then authorizes the user with an available VLAN in the VLAN pool. If all VLANs in the VLAN pool are locked, the device authorizes the user with the default VLAN for the interface through which the user goes online.

Prerequisites

For wired users, you must run the **assignment hash** command to set the VLAN assignment algorithm to hash. For wireless users, the device must support the WLAN-AC function.

Precautions

For wireless users, you can also run the **dhcp update vlan assignment interval** command to configure the interval at which the VLAN pool module receives such a notification from the DHCP module. Otherwise, the default interval is used.

Before configuring this function for wired users, run the **dhcp update vlan assignment** command to enable the function of reassigning VLANs in the VLAN pool. Otherwise, the function of locking a specific VLAN does not take effect.

Before enabling the function of reassigning VLANs in the VLAN pool for wired users, you need to enable DHCP snooping on the interface through which users go online.

Authentication access devices in the policy association scenario do not support this function.

Example

Configure the device to lock a VLAN after the VLAN pool module receives a notification from the DHCP module five times, indicating that wired users fail to obtain IP addresses from the IP address pool for the VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] assignment hash
[HUAWEI-vlan-pool-test] dhcp update vlan assignment
[HUAWEI-vlan-pool-test] dhcp update vlan assignment threshold 5
```

Configure the device to lock a VLAN after the VLAN pool module receives a notification from the DHCP module five times within 4 minutes, indicating that wireless users fail to obtain IP addresses from the IP address pool for the VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] dhcp update vlan assignment threshold 5
[HUAWEI-vlan-pool-test] dhcp update vlan assignment interval 4
```

13.1.57 dns (service scheme view)

Function

The **dns** command configures the primary or secondary DNS server in a service scheme.

The **undo dns** command cancels the configuration of the primary or secondary DNS server in a service scheme.

By default, no primary or secondary DNS server is configured in a service scheme.

Format

dns *ip-address* [**secondary**]

undo dns [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the DNS server.	The value is a valid unicast address in dotted decimal notation.
secondary	Indicates the secondary DNS server.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

If no DNS server is specified when a local address pool, DHCP server, or RADIUS server assigns IP addresses to users, the DNS server configured in the service scheme view is used.

Example

Set the IP address of the primary DNS server in the service scheme **svcscheme1** to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme svcscheme1
[HUAWEI-aaa-service-svcscheme1] dns 10.10.10.1
```

Set the IP address of the secondary DNS server in the service scheme **svcscheme1** to 10.10.20.1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme svcscheme1
[HUAWEI-aaa-service-svcscheme1] dns 10.10.20.1 secondary
```

13.1.58 domain (AAA view)

Function

The **domain** command creates a domain and displays its view.

The **undo domain** command deletes a domain.

By default, the device has two domains: **default** and **default_admin**. The two domains can be modified but cannot be deleted.

Format

domain *domain-name* [**domain-index** *domain-index*]

undo domain *domain-name*

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a domain.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces or the following symbols: * ? ". The value cannot be - or --.
domain-index *domain-index*	Specifies the index of a domain.	The value is an integer that ranges from 0 to 31.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device can manage users through domains. A domain is the minimum user management unit. A domain name can be an ISP name or the name of a service provided by an ISP. A domain can use the default authorization attribute, and be configured with a RADIUS template and authentication and accounting schemes.

If the domain to be configured already exists, the **domain** command displays the domain view.

Running the **undo domain** command to delete a domain will cause online users that belong to this domain to go offline. Confirm the operation before running this command.

Prerequisites

To perform AAA for access users, you need to apply the authentication schemes, authorization schemes, and accounting schemes in the domain view. Therefore, authentication, authorization, and accounting schemes must be configured in the AAA view in advance.

Precautions

- The domain **default** is a global default common domain for user access, for example, NAC. By default, the domain is activated, and is bound to the

authentication scheme **radius** and accounting scheme **default**, but is not bound to any authorization scheme.

- The domain **default_admin** is a global default management domain for users who log in to the device through HTTPS, SSH, Telnet, and the Web system, namely, administrators. By default, the domain is activated, and is bound to the authentication scheme **default** and accounting scheme **default**, but is not bound to any authorization scheme.

Example

Specify the domain named **domain1** and access the domain view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain domain1
[HUAWEI-aaa-domain-domain1]
```

13.1.59 domain (system view)

Function

The **domain** command configures a global default domain.

The **undo domain** command restores the default setting.

By default, there are two global default domains: common domain **default** and administrative domain **default_admin**. The former is used as the global default domain of access users, while the latter as the global default domain of administrators.

Format

Common domain **default**:

domain *domain-name*

undo domain

Administrative domain **default_admin**:

domain *domain-name* **admin**

undo domain admin

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a global default domain.	The domain must already exist.

Parameter	Description	Value
admin	Configures a domain for administrators. If this parameter is not specified, the domain for common access users is configured.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the global default domain is configured, a user must be managed by the global default domain if their domain cannot be identified.

Precautions

You must create a domain before configuring the domain as the global default domain.

Example

Create domain **abc** and configure it as the global default common domain.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain abc
[HUAWEI-aaa-domain-abc] quit
[HUAWEI-aaa] quit
[HUAWEI] domain abc
```

13.1.60 domain-location

Function

The **domain-location** command configures the position of a domain name.

The **undo domain-location** command restores the default position of a domain name.

By default, the domain name in the AAA view is placed behind the domain name delimiter, and no position is configured in the authentication profile view.

NOTE

Only S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command in the authentication profile view.

Format

domain-location { **after-delimiter** | **before-delimiter** }

undo domain-location

Parameters

Parameter	Description	Value
after-delimiter	Indicates that the domain name is placed behind the domain name delimiter.	-
before-delimiter	Indicates that the domain name is placed before the domain name delimiter.	-

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

The format of a user name is **user name@domain name**. If **before-delimiter** is specified, the format **domain name@user name** is used.

You can use the **domain-location** command only when there is no online user.

Precautions

If you run the **domain-location** command in the AAA view, the position of a domain is configured globally and the configuration takes effect for all users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the authentication profile, the

configuration takes effect for only the users connected to this authentication profile.

Example

Configure the domain name before the domain name delimiter.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain-location before-delimiter
```

13.1.61 domain-name-delimiter

Function

The **domain-name-delimiter** command configures a domain name delimiter.

The **undo domain-name-delimiter** command restores the default domain name delimiter.

By default, the domain name delimiter in the AAA view is @, and no delimiter is available in the authentication profile view.

NOTE

Only S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command in the authentication profile view.

Format

domain-name-delimiter *delimiter*

undo domain-name-delimiter

Parameters

Parameter	Description	Value
delimiter	Specifies a domain name delimiter of only one bit.	The value can only be one of the following characters: \ / : < > | @ ' %.

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

Different AAA servers may use different domain name delimiters. To ensure that an AAA server obtains the correct user name and domain name, configure the same domain name delimiter on the device and the AAA server.

For example, if the domain name delimiter is %, the user name of **user1** in the domain **dom1** is **user1%dom1** or **dom1%user1**.

Precautions

Before using the **domain-name-delimiter** command, ensure that no local user exists.

If you run the **domain-name-delimiter** command in the AAA view, the domain name delimiter is configured globally and the configuration takes effect for all users.

The delimiter for a security string cannot be the same as the domain name delimiter.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

Example

Configure the domain name delimiter as / in the AAA view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain-name-delimiter /
```

13.1.62 domainname-parse-direction

Function

The **domainname-parse-direction** command configures the direction in which a domain name is parsed.

The **undo domainname-parse-direction** command restores the default direction in which a domain name is parsed.

By default, the domain name is parsed in the AAA view from left to right, and no direction is configured in which a domain name is parsed.

NOTE

Only S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command in the authentication profile view.

Format

domainname-parse-direction { **left-to-right** | **right-to-left** }

undo domainname-parse-direction

Parameters

Parameter	Description	Value
left-to-right	Parses a domain name form left to right.	-
right-to-left	Parses a domain name form right to left.	-

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

In AAA implementations, users belong to different domains. A network access server (NAS) centrally manages users in a domain. During a user's login, the NAS parses the entered user name. A user is authenticated only when the user has the correct user name and domain name. When configuring an AAA scheme, run the **domainname-parse-direction** { **left-to-right** | **right-to-left** } command to configure the direction in which a domain name is parsed.

Assume that the user name is **username@dom1@dom2**.

- If the **domain-location** command configures the domain name behind the domain name delimiter:
  - When **left-to-right** is specified, the user name is **username** and the domain name is **dom1@dom2**.
  - When **right-to-left** is specified, the user name is **username@dom1** and the domain name is **dom2**.
- If the **domain-location** command configures the domain name before the domain name delimiter:
  - When **left-to-right** is specified, the user name is **dom1@dom2** and the domain name is **username**.
  - When **right-to-left** is specified, the user name is **dom2** and the domain name is **username@dom1**.

Precautions

If you run the **domainname-parse-direction** command in the AAA view, the direction in which a domain name is parsed is configured globally and the configuration takes effect for all users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

Example

Configure the device to parse a domain name from right to left in the AAA view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domainname-parse-direction right-to-left
```

13.1.63 hash mac-vlan lease

Function

The **hash mac-vlan lease** command sets the aging time of user entries in a VLAN pool.

The **undo hash mac-vlan lease** command restores the default configuration.

By default, the aging time of user entries in a VLAN pool is 8 days.

Format

hash mac-vlan lease { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo hash mac-vlan lease

Parameters

Parameter	Description	Value
day *day*	Specifies the aging time, in days.	The value is an integer in the range from 0 to 999, in days. The default value is 8 days.
hour *hour*	Specifies the aging time, in hours.	The value is an integer in the range from 0 to 23, in hours. The default value is 0.
minute *minute*	Specifies the aging time, in minutes.	The value is an integer in the range from 0 to 59, in minutes. The default value is 0.
unlimited	Indicates that entries will not be aged.	-

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

To ensure that an offline user still belongs to the original VLAN when the user goes online again, the device records the mapping between the user MAC address and the VLAN. When the user goes online again, the system searches for a matching entry to determine the VLAN to which the user once belonged. If the entry exists and the number of users in the VLAN does not reach the upper limit, the user still belongs to the original VLAN. If the entry does not exist or the number of users in the VLAN reaches the upper limit, the system assigns another available VLAN to the user. To adjust the aging time of entries, run the **hash mac-vlan lease** command.

NOTE

- The **hash mac-vlan lease** command takes effect only for users authorized a VLAN pool.
- The **hash mac-vlan lease** command takes effect only when the VLAN assignment algorithm of a VLAN pool is **hash**.
- The aging time takes effect only for entries of offline users.
- The configured aging time must be greater than or equal to 10 minutes.

Example

Set the aging time of offline user entries in a VLAN pool to 7 days.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] hash mac-vlan lease day 7
```

13.1.64 idle-cut (service scheme view)

Function

The **idle-cut** command enables the idle-cut function for domain users and sets the idle-cut parameters.

The **undo idle-cut** command disables the idle-cut function.

By default, the idle-cut function is disabled for domain users.

Format

idle-cut *idle-time flow-value* [**inbound** | **outbound**]

undo idle-cut

Parameters

Parameter	Description	Value
idle-time	Specifies the period in which an idle user can stay online.	The value is an integer that ranges from 1 to 1440, in minutes.
flow-value	Specifies the traffic threshold for idle-cut function. When the traffic of a user stays below this threshold for a certain period, the device considers that the user is in idle state.	The value is an integer that ranges from 0 to 4294967295, in Kbytes.
inbound	Indicates that the idle-cut function takes effect for only upstream traffic of users.	-
outbound	Indicates that the idle-cut function takes effect for only downstream traffic of users. **NOTE** If neither **inbound** nor **outbound** is specified, the idle-cut function takes effect for both upstream and downstream traffic. In addition, if only the traffic in one direction meets the idle-cut condition (the traffic volume is less than the threshold specified by *flow-value* within the time specified by *idle-time*), the idle-cut function takes effect and the user connection is disconnected.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user uses no or a little network traffic for a long time, the user still occupies certain bandwidth, which reduces access rate of other users. The idle-cut function disconnects the users whose traffic volume stays below the traffic threshold within the idle time, to save resources and improve service experience of other users.

Precautions

- The **idle-cut** command configured in the service scheme view takes effect only for wireless users.
- When idle-cut in the service scheme view and RADIUS attribute 28 (Idle-Timeout) delivered by the remote RADIUS server exist simultaneously, RADIUS

attribute 28 has a higher priority. RADIUS attribute 28 can be used together with the traffic and direction configured using this command.

Example

Enable the idle-cut function for the domain, and set the idle time to 1 minute and the traffic threshold to 10 Kbytes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] idle-cut 1 10
```

13.1.65 local-aaa-user wrong-password

Function

The **local-aaa-user wrong-password** command enables local account locking function and sets the retry interval, consecutive incorrect password attempts, and locking duration.

The **undo local-aaa-user wrong-password** command disables local account locking function.

By default, the local account locking function is enabled, retry interval is 5 minutes, maximum number of consecutive incorrect password attempts is 3, and account locking period is 5 minutes.

Format

local-aaa-user wrong-password retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

undo local-aaa-user wrong-password

Parameters

Parameter	Description	Value
retry-interval *retry-interval*	Specifies the retry interval of a local account.	The value is an integer that ranges from 5 to 65535, in minutes.
retry-time *retry-time*	Specifies the consecutive incorrect password attempts.	The value is an integer that ranges from 3 to 65535.
block-time *block-time*	Specifies the local account locking duration. In actual application, there is a one minute difference in locking time.	The value is an integer that ranges from 5 to 65535, in minutes.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the following scenarios:

- The command locks a local account to improve password security of the local user. If the password is entered incorrectly more than a certain number of times within the given retry period, the account is locked. The device does not authenticate the user when the account is locked.
- The command locks a local account to ensure that the password will not be cracked by a brute force from a malicious user. When attempting to change the password, if the original password is entered incorrectly more than a certain number of times within the given retry period, the account is locked. The user cannot modify the password when the account is locked.

Follow-up Procedure

After a local account is locked, you can run the **local-user** *user-name* **state active** command to unlock the local account.

Precautions

Only entering the incorrect password can lock the account. Other local authentication failures will not lock the account.

When the number of login failures or initial password change failures of the local user does not reach the limit specified using the **local-aaa-user wrong-password** command, the user is not locked. In this case, if the limit is changed using the **local-aaa-user wrong-password** command and the new limit is smaller than the number of login failures or initial password change failures of the user, the user still has a chance to log in to the device or change the password.

Example

Enable local account locking, and set the authentication retry interval to 5 minutes, maximum number of consecutive incorrect password attempts to 3, and account locking period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time 5
```

13.1.66 local-user

Function

The **local-user** command creates a local user and sets parameters of the local user.

The **undo local-user** command deletes a local user.

By default, no local user is created. The privilege level of a new local user is 0, and no service type is configured.

Format

local-user *user-name* { **password** { **cipher** | **irreversible-cipher** } *password* [**old-password** *old-password*] | **access-limit** *max-number* | **ftp-directory** *directory* | **idle-timeout** *minutes* [*seconds*] | **privilege level** *level* | **state** { **block** | **active** } | **user-group** *group-name* } *

local-user *user-name* **http-directory** *directory*

undo local-user *user-name* [**access-limit** | **ftp-directory** | **http-directory** | **idle-timeout** | **privilege level** | **user-group**]

Parameters

Parameter	Description	Value
user-name	Specifies the user name. If the user name contains a domain name delimiter such as @, the character before @ is the user name and the character behind @ is the domain name. If the value does not contain @, the entire character string is the user name and the domain name is the default one.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

Parameter	Description	Value

		NOTE
		• During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		• Note the following when configuring case sensitivity for user names:
		  • Only the user name is case-sensitive and the domain name is case-insensitive.
		  • For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  • When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user

Parameter	Description	Value
password { **cipher** | **irreversible-cipher** } *password*	Specifies the password of a local user. • The **cipher** parameter indicates that the user password is encrypted using the reversible encryption algorithm. Unauthorized users can obtain the plain text by using the corresponding decryption algorithm, leading to low security. When the **cipher** parameter is specified, the AES reversible encryption algorithm is used. • The **irreversible-cipher** parameter indicates that the user password is encrypted using the irreversible encryption algorithm. Unauthorized users cannot obtain the plain text by using the decryption algorithm, ensuring user security. When the **irreversible-cipher** parameter is specified, the Scrypt irreversible encryption algorithm is used.	The value is a case-sensitive character string without question marks (?), single quotation marks ('), and spaces. • If the **cipher** parameter is specified, the value of *password* can be a cleartext password of 8 to 128 characters or a ciphertext password of 48, 68, 88, 108, 128, 148, 168, or 188 characters. • If the **irreversible-cipher** parameter is specified, the value of *password* can be a cleartext password of 8 to 128 characters or a ciphertext password of 68 characters. A simple password may bring security risks. The cleartext password entered by a user must contain at least two types of the following characters: uppercase letters, lowercase letters, digits, and special characters. In addition, the password cannot repeat or reverse the user name.

Parameter	Description	Value
	NOTE • It is recommended that you set the user password when creating a user. The interaction method using the **local-user password** command is recommended. • If a user is allowed to encrypt the local user password using the irreversible encryption algorithm, the device does not support CHAP authentication for the user. • In V200R019C10 and later versions, if the local user password is encrypted using irreversible algorithms, the **password** configuration of the local user will be lost and cannot be restored after a downgrade to a version earlier than V200R019C10.	
old-password *old-password*	Specifies the old password of a local user.	The value is a case-sensitive character string without question marks (?), single quotation marks ('), and spaces. The value is a string of 1 to 128 characters in plain text.
access-limit *max-number*	Specifies the number of connections that can be created with a specified user name. If this parameter is not specified, a user can establish a maximum of 4294967295 connections by default.	The value is an integer that ranges from 1 to 4294967295. The actual number of connections is the smaller value between *max-number* and the maximum number of users of a specific type on different models.

Parameter	Description	Value
ftp-directory *directory*	Specifies the directory that an FTP user is allowed to access. If this parameter is not specified, the FTP directory of the local user is empty. The device will check whether the default FTP directory is configured using the **set default ftp-directory** command. If no FTP directory exists, FTP users cannot log in to the device. **NOTE** Ensure that the configured FTP directory is an absolute path; otherwise, the configuration does not take effect.	The value is a string of 1 to 64 case-sensitive characters without spaces.
http-directory *directory*	Specifies the directory that HTTP users are allowed to access. If this parameter is not specified, the HTTP directory of the local user is empty.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Parameter	Description	Value
idle-timeout *minutes* [*seconds*]	Specifies the timeout period for disconnection of the user. • *minutes* is the period when the user interface is disconnected in minutes. • *seconds* is the period when the user interface is disconnected in seconds. If this parameter is not specified, the device uses the idle timeout interval configured by the **idle-timeout** command in the user interface view. If *minutes* [*seconds*] is set to **0 0**, the idle disconnection function is disabled. **NOTICE** If the idle timeout interval is set to 0 or a large value, the terminal will remain in the login state, resulting in security risks. You are advised to run the **lock** command to lock the current connection.	*minutes*: The value is an integer ranging from 0 to 35791 minutes. *seconds*: The value is an integer ranging from 0 to 59 seconds.
privilege level *level*	Specifies the privilege level of a local user. After logging in to the device, a user can run only the commands of the same privilege level or lower privilege levels. **NOTE** If this parameter is not specified, the privilege level of a local user is 0. The permission of API users is not controlled by this parameter. Therefore, you do not need to configure this parameter.	The value is an integer that ranges from 0 to 15. The greater the value, the higher the privilege level of a user.

Parameter	Description	Value
state { **active** | **block** }	Indicates the state of a local user. • **active** indicates that a local user is in active state. The device accepts and processes the authentication request from the user, and allows the user to change the password. • **block** indicates that a local user is in blocking state. The device rejects the authentication request from the user and does not allow the user to change the password. If a user has established a connection with the device, when the user is set in blocking state, the connection still takes effect but the device rejects subsequent authentication requests from the user. If this parameter is not specified, the status of a local user is active.	-
user-group *group-name*	Specifies the name of a user group. **NOTE** This parameter is supported only by the switches in NAC common mode.	The value is a string of 1 to 64 case-sensitive characters without spaces. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To facilitate device maintenance, create a local user and set parameters such as the password, FTP directory and user privilege level.

Prerequisites

Before adding a local user to a user group, ensure that the user group has been created using the **user-group** command.

Precautions

- For device security purposes, change the password periodically.
- Security risks exist if the user login mode is set to Telnet or FTP. You are advised set the user login mode to STelnet or SFTP and set the user access type to SSH.

  When a device starts without any configuration, HTTP uses the randomly generated self-signed certificate to support HTTPS. The self-signed certificate may bring risks. Therefore, you are advised to replace it with the officially authorized digital certificate.
- After a local administrator logs in to the device, the administrator can create, modify, or delete attributes of other local users of the same or a lower privilege level. The attributes include the password, user privilege level, maximum number of access users, and account validity period.

  After you change the rights (for example, the password, FTP directory, idle timeout interval, or status) of a local account, the rights of online users do not change, and the change takes effect for new online users.

  A local administrator who goes online using local authorization will go offline after the user privilege level of the administrator is changed. If no authorization template is configured, a local administrator who goes online using local authentication will also go offline after the user privilege level of the administrator is changed.
- Online users cannot be deleted. When the user is offline or the **cut access-user username** *user-name* command is executed in the AAA view to disconnect the user, delete the user.
- The user name function may be invalid due to improper configuration of the domain name delimiter.
- One user group can be used by multiple local users. However, a local user belongs to only one user group. If the user groups have been configured for the local user and in the service template, only the user group configured for the local user takes effect. The user groups that are used by a local user or an online user cannot be deleted.
- After the device is restarted, the locked account is automatically unlocked.
- During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

Example

Create a local user **user1**, and set the domain name to **vipdomain**, the password to YsHsjx_202206 in ciphertext, the maximum number of connections to 100, and the idle timeout interval to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain password irreversible-cipher YsHsjx_202206 access-limit 100 idle-timeout 10
```

13.1.67 local-user change-password

Function

The **local-user change-password** command enables local users to change their passwords.

Format

local-user change-password

Parameters

None

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If you are a low-level administrator, to ensure security of the password, you can run the **local-user change-password** command in the user view to change your password after passing the authentication.

Precautions

- To modify the password, a local user must enter the old password.
- Only the user who passes local authentication can change the password using this command. After a local user successfully changes the password, the user needs to enter the new password for authentication upon the next login.
- The **local-user change-password** command is used to change the password of a local user. It does not save the configuration, but the result of changing the password is saved through the **local-user password** command. If the server does not receive old password, new password, or confirmed password from the user within 30 seconds, it terminates the password change process. When the user presses **Ctrl+C** to cancel password change, the password change process is terminated.

- A simple local user password may bring security risks. When a local user changes the password, the password must be a string of 8 to 128 characters and contain at least two types of the following characters: uppercase letters, lowercase letters, digits, and special characters. In addition, the password cannot repeat or reverse the user name.
- For device security purposes, change the password periodically.
- During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

Example

Configure a user that passes local authentication to change the password.

```
<HUAWEI> local-user change-password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numerals and special characters.
Plese enter old password:
Please enter new password:
Please confirm new password:
Info: The password is changed successfully.
```

13.1.68 local-aaa-user change-password verify

Function

The **local-aaa-user change-password verify** command enables the function of verifying the original password when local administrators change their own passwords.

The **undo local-aaa-user change-password verify** command disables the function of verifying the original password when local administrators change their own passwords.

By default, the function of verifying the original password is enabled when local administrators change their own passwords.

Format

local-aaa-user change-password verify

undo local-aaa-user change-password verify

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

By default, when local administrators change their passwords using the **local-aaa-user change-password verify** command in the AAA view, the administrators need to enter the original password for verification. During management and O&M, you can determine whether to run the **undo local-aaa-user change-password verify** command to disable password verification as required.

- If the **command-privilege level rearrange** command has been run in the system view, levels of level-2 and level-3 commands are increased to 10 and 15 in a batch, respectively. After the **undo local-aaa-user change-password verify** command is run, the system does not verify the original password only when level-15 administrators change their own passwords.
- If the **command-privilege level rearrange** command is not run in the system view and the **undo local-aaa-user change-password verify** command has been run, the system does not verify the original password when administrators of levels 3 to 15 change their own passwords, and the system still needs to verify the original password when administrators of other levels change their own passwords.

Example

Enable the function of verifying the original password when local administrators change their own passwords.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] undo local-aaa-user change-password verify
Warning: This command will disable the function of verifying the old password when administrators changes their own passwords. Continue?[Y/N]
```

13.1.69 local-user device-type

Function

The **local-user device-type** command configures the type of terminals allowed to access the network.

The **undo local-user device-type** command deletes the type of terminals allowed to access the network.

By default, the type of terminals allowed to access the network is not configured.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

local-user *user-name* **device-type** *device-type* &<1-8>

undo local-user *user-name* **device-type**

Parameters

Parameter	Description	Value

user-name	Specifies the name of a local user.
	When querying and modifying the user account, you can use the wildcard *, for example, *@isp, user@*, and *@*.
		The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		• During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		• Note the following when configuring case sensitivity for user names:
		  • Only the user name is case-sensitive and the domain name is case-insensitive.
		  • For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  • When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

device-type	Specifies a terminal type.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

You can run the **local-user device-type** command to configure the type of terminals allowed to access the network. In local authentication and authorization, the device checks whether a terminal is allowed to access the network. If so, the device checks the user name and password of the terminal.

Example

Set the type of the terminal that local user **hello** uses to access the network to **iphone**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user hello device-type iphone
```

13.1.70 local-user expire-date

Function

The **local-user expire-date** command sets the expiration date of a local account.

The **undo local-user expire-date** command restores the default expiration date of a local account.

By default, a local account is permanently valid.

Format

local-user *user-name* **expire-date** *expire-date*

undo local-user *user-name* **expire-date**

Parameters

Parameter	Description	Value

user-name	Specifies a local account.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		• During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		• Note the following when configuring case sensitivity for user names:
		  • Only the user name is case-sensitive and the domain name is case-insensitive.
		  • For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  • When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

expire-date	Specifies the expiration date of the local account.	The value is in YYYY/MM/DD format. YYYY specifies the year, MM specifies the month, and DD specifies the day. The value ranges from 2000/1/1 to 2099/12/31.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a local account is created, the account has no expiration date by default. You can run the **local-user expire-date** command to set the expiration date of a local

account. When the expiration date is reached, the account expires. This configuration enhances network security.

Precautions

- For example, if the expiration date of the local account is set to 2013-10-1, the account becomes invalid at 00:00 on 2013-10-1.
- This function takes effect only for users who go online after this function is successfully configured.

Example

Set the expiration date of local account **hello@163.net** to 2013/10/1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user hello@163.net expire-date 2013/10/1
```

13.1.71 local-user ftp-privilege

Function

The **local-user ftp-privilege** command configures the FTP permissions for a local user.

The **undo local-user ftp-privilege** command restores the default FTP permissions of a local user.

By default, FTP permissions of a local user are the read, write, and execute permissions.

Format

local-user *user-name* **ftp-privilege** [*directoryfilename*] { **read** | **write** | **execute** }*

undo local-user *user-name* **ftp-privilege** [*directoryfilename*]

Parameters

Parameter	Description	Value
user-name	Specifies the user name of a local user. If the user name contains a delimiter of at sign (@), the character string before the at sign is the user name and the character string following the at sign is the domain name. If the user name does not contain the at sign, the entire character string represents the user name and the domain name is the default one.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisks (*), double quotation marks ("), or question marks (?).
directoryfilename	Specifies the directory or file name of the FTP operation.	The value is a string of 1 to 160 case-sensitive characters. It cannot contain spaces.
read	Indicates that local users have only read permission.	-
write	Indicates that local users have only write permission.	-
execute	Indicates that local users have only execute permission.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To facilitate device maintenance, the administrator can run this command to configure FTP permissions for local users so that different users have different permissions to operate different directories or files.

Different FTP commands require different FTP permissions:

- The read permission is required for running the **pwd**, **dir**, and **ls** commands.
- The write permission is required for running the **mkdir**, **rmdir**, **delete**, **put**, and **mpu** commands.
- The execute permission is required for running the **cd**, **cdup**, **get**, **ascii**, and **binary** commands.
- Running the **mget** command must meet the following requirements: The execute permission is required for the current directory; the read permission is required for operating all files (including the files matching the wildcard *); the execute permission is required for running the **mget** command on each file.

Precautions

- If *directoryfilename* is not specified, this command configures the permissions on the FTP directory that local users can access.
- Directory matching complies with the longest match principle. For example, if both the **local-user 1 ftp-privilege flash:/logfile/ read** and **local-user 1 ftp-privilege flash:/logfile/log.log execute** commands are configured on the device, the local user has the execute permission on the file **flash:/logfile/log.log** and the read permission on other files in the directory **flash:/logfile/**. If no permission is configured for a specified directory or file, the directory or file inherits the permission of the upper-level directory.
- The specified directory or file name must be an absolute path.For example, "flash:/my/test/"

Example

Grant the read permission on the FTP directory to the local user **user1@vipdomain**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain ftp-privilege read
```

Grant the read and write permissions on the directory **logfile** to the local user **user1@vipdomain**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain ftp-privilege flash:/logfile/ read write
```

13.1.72 local-user password

Function

The **local-user password** command configures a password for a local account.

By default, the password of a local account is empty.

Format

local-user *user-name* **password**

NOTE

This command is an interactive command. After you enter **local-user** *user-name* **password** and press **Enter**, you can set the password as prompted. The local user password is a string of 8 to 128 case-sensitive characters.

Parameters

Parameter	Description	Value

user-name	Specifies the local user name.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		• During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		• Note the following when configuring case sensitivity for user names:
		  • Only the user name is case-sensitive and the domain name is case-insensitive.
		  • For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  • When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

If no password is configured when a local user is created, the password is empty, and the local user cannot log in to the device.

NOTICE

A simple local user password may bring security risks. The user password must consist of two types of characters, including uppercase letters, lowercase letters, digits, and special characters. In addition, the password cannot repeat or reverse the user name.

Example

Set the password to **YsHsjx_202206** for the local account **hello@163.net**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user hello@163.net password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, i
ncluding lowercase letters, uppercase letters, numerals and special characters.
Please enter password:              //Enter the password
YsHsjx_202206
Please confirm password:            //Confirm the password YsHsjx_202206
Info: Add a new user.
```

13.1.73 local-user password change-offline enable

Function

The **local-user password change-offline enable** command enables the interactive confirmation function when a local administrator changes the password.

The **undo local-user password change-offline enable** command disables the interactive confirmation function when a local administrator changes the password.

By default, the interactive confirmation function is enabled when a local administrator changes the password.

Format

local-user password change-offline enable

undo local-user password change-offline enable

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

By default, when a local administrator runs the **local-user** *user-name* **password** command in the AAA view to change the password, the device is enabled to interact with the user. In this case, the device displays a message indicating that the user account will be deregistered and the user needs to log in again. During management and O&M, you can determine whether to run the **undo local-user password change-offline enable** command to disable the interactive confirmation function as required.

Example

Enable the interactive confirmation function when a local administrator changes the password.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user password change-offline enable
[HUAWEI-aaa] local-user admin password irreversible-cipher YsHsjx_202206
Warning: The user using this account will be logged out, and needs to log in again. Do you want to continue? [Y/N]y
```

13.1.74 local-aaa-user password policy access-user

Function

The **local-aaa-user password policy access-user** command enables the password policy for local access users and enters the local access user password policy view.

The **undo local-aaa-user password policy access-user** command disables the password policy of local access users.

By default, the password policy of local access users is disabled.

Format

local-aaa-user password policy access-user

undo local-aaa-user password policy access-user

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

After a local user is created using the **local-user** command, the minimum length and complexity of the password are limited. If you want to improve password

security, run this command to configure password policy. The new password cannot be the same as any previously used password stored on the device.

Example

Enable the local access user password policy and enter the local access user password policy view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy access-user
[HUAWEI-aaa-lupp-acc]
```

13.1.75 local-aaa-user password policy administrator

Function

The **local-aaa-user password policy administrator** command enables the password policy for local administrators and enters the local administrator password policy view.

The **undo local-aaa-user password policy administrator** command disables the password policy of local administrators.

By default, the password policy for local administrators is enabled.

Format

local-aaa-user password policy administrator

undo local-aaa-user password policy administrator

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a local user is created using the **local-user** command, the minimum length and complexity of the password are limited. If you want to improve password security, you can run the following commands to configure the password policy for local administrators:

- Run the **password expire** command to set the password validity period.
- Run the **password alert before-expire** command to set the password expiration prompt days.

- Run the **password alert original** command to enable the device to prompt users to change initial passwords.
- Run the **password history record number** command to set the maximum number of previously used passwords recorded for each user.

Precautions

After the **undo local-aaa-user password policy administrator** command is executed, the administrator password policy will be disabled, causing a security risk.

After the device is restored to factory settings, the password policy for local administrators is enabled by default.

When the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **local-aaa-user password policy administrato** command to enable the password policy for local administrators.
- Run the **password expire 0** command to configure the passwords of local administrators to be permanently valid.
- Run the **password history record number 0** command to configure the device not to check whether a changed password of a local administrator is the same as any historical password.

Example

Enable the password policy for local administrators and enter the local administrator password policy view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin]
```

13.1.76 local-user service-type

Function

The **local-user service-type** command sets the access type for a local user.

The **undo local-user service-type** command restores the default access type for a local user.

By default, a local user cannot use any access type.

Format

local-user *user-name* **service-type** { **8021x** | **api** | **ftp** | **http** | **ppp** | **ssh** | **telnet** | **terminal** | **web** | **x25-pad** } *

undo local-user *user-name* **service-type**

NOTE

All models support the api parameter, except S1720GW-E, S1720GWR-E, and S1720X-E.

Parameters

Parameter	Description	Value
user-name	Specifies a user name. If the user name contains a domain name delimiter such as @, the character before @ is the user name and the character behind @ is the domain name. If the value does not contain @, the entire character string is the user name and the domain name is the default one.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

Parameter	Description	Value

		NOTE
		● During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		● Note the following when configuring case sensitivity for user names:
		  ● Only the user name is case-sensitive and the domain name is case-insensitive.
		  ● For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  ● When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Parameter	Description	Value
8021x	Indicates an 802.1X user.	-
api	Indicates an API user, which is typically used for NETCONF access. **NOTE** If the access type of a user is API, the user name cannot be set to **root**.	-
ftp	Indicates an FTP user.	-
http	Indicates an HTTP user, which is usually used for web system login.	-
ppp	Indicates a PPP user.	-
ssh	Indicates an SSH user.	-
telnet	Indicates a Telnet user, which is usually a network administrator.	-
terminal	Indicates a terminal user, which is usually a user connected using a console port.	-
web	Indicates a Portal authentication user.	-
x25-pad	Indicates an X25-PAD user. **NOTE** Currently, the device does not support X25-PAD.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device can manage access types of local users. After you specify the access type of a user, the user can successfully log in only when the configured access type is the same as the actual access type of the user.

Local users have the following access types:

- Administrative: api, FTP, HTTP, SSH, Telnet, x25-pad, and Terminal
- Common: 802.1X, ppp, and web

Precautions

- When MAC authentication users use AAA local authentication, the device does not match or check the access type of local users. However, the access type must be configured; otherwise, local authentication for MAC address authentication users fails.
- Security risks exist if the user login mode is set to Telnet or FTP. You are advised set the user login mode to STelnet or SFTP and set the user access type to SSH.

  When a device starts without any configuration, HTTP uses the randomly generated self-signed certificate to support HTTPS. The self-signed certificate may bring risks. Therefore, you are advised to replace it with the officially authorized digital certificate.
- Common access types cannot be configured together with administrative access types.

  The API access type cannot be configured together with other access types.

  If a user has been created and the password uses an irreversible encryption algorithm, the access type can only be set to an administrative one.

  If a user has been created and the password uses a reversible encryption algorithm, the access type can be set to an administrative or common one. When the access type is set to an administrative one, the encryption algorithm of the password is automatically converted into an irreversible encryption algorithm.

Example

Set the access type of the local user **user1@vipdomain** to SSH.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain service-type ssh
```

13.1.77 local-user time-range

Function

The **local-user time-range** command sets the access permission time range for a local user.

The **undo local-user time-range** command deletes the access permission time range for a local user.

By default, a local account can access the network anytime.

Format

local-user *user-name* **time-range** *time-name*

undo local-user *user-name* **time-range**

Parameters

Parameter	Description	Value

user-name	Indicates the local account.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		• During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		• Note the following when configuring case sensitivity for user names:
		  • Only the user name is case-sensitive and the domain name is case-insensitive.
		  • For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  • When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

time-name	Indicates the access permission time range of the local account. *time-name* specifies the name of the access permission time range.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word **all** cannot be specified as a time range name.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Use Scenario

After a local account is created, the account has no expiration date by default. To restrict the network access time of a local account, run the **local-user time-range** command. After the command is executed, the account can access network resources only in the specified time range.

Prerequisite

The time range has been created using the **time-range** command.

Precautions

If you run the **local-user time-range** and **local-user expire-date** commands in the AAA view multiple times, only the latest configuration takes effect.

After the access permission time range of an online local user is changed, the access permission time range of the user will take effect only when the user goes online next time.

Example

Set the access permission time segment of local account hello@163.net to 9:00-18:00 from Monday to Friday.

```
<HUAWEI> system-view
[HUAWEI] time-range test 9:00 to 18:00 working-day
[HUAWEI] aaa
[HUAWEI-aaa] local-user hello@163.net time-range test
```

13.1.78 local-user user-type netmanager

Function

The **local-user user-type netmanager** command configures a local user as the NMS user.

The **undo local-user user-type netmanager** command cancels to configure a local user as the NMS user.

By default, no local user is configured as the NMS user.

Format

local-user *user-name* **user-type netmanager**

undo local-user *user-name* **user-type netmanager**

Parameters

Parameter	Description	Value

user-name	Specifies a user name.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		• During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		• Note the following when configuring case sensitivity for user names:
		  • Only the user name is case-sensitive and the domain name is case-insensitive.
		  • For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  • When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a VTY user logging in to the device is an NMS user, you need to run this command to set the user type. When the number of login VTY users has reached the maximum, an NMS user can log in using the reserved VTY numbers 16-20. The NMS user is allowed to log in to the device only after passing the AAA local authentication.

Prerequisite

The local user has been created using the **local-user** command. This user must pass the AAA local authentication.

Example

Configure the local user user1@vipdomain as the NMS user.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain password cipher YsHsjx_202206
[HUAWEI-aaa] local-user user1@vipdomain user-type netmanager
```

13.1.79 load security weak-password-dictionary

Function

The **load security weak-password-dictionary** command loads a weak password dictionary.

Format

load security weak-password-dictionary *filename*

Parameters

Parameter	Description	Value
filename	Specifies the name of a weak password dictionary file.	The value is a string of case-insensitive characters, including uppercase letters, lowercase letters, digits, and special characters. It cannot contain spaces. The value is a string of 1 to 64 characters (including the file name extension). The following special characters are not supported: ~ ? * / \ : " | < > [ ]. The first or last character cannot be a period (.). The file name extension must be .txt.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

No weak password is preset on the device by default. You can run this command to load a weak password dictionary to the memory for weak password check during the configuration of the management plane password.

Prerequisites

Before loading a weak password dictionary, make a .txt weak password dictionary file and upload it to the device. Otherwise, the weak password dictionary file fails to be loaded.

Precautions

1. When you run this command, the system checks the file validity:
   - The system checks whether the file exists. Only the files in the directory where the .cc package is located can be verified. If the file does not exist, the command fails to be executed.
   - The system checks whether the file size is less than or equal to 1 MB. If the file size is greater than 1 MB, the command fails to be executed.
   - The system checks whether the file is a .txt file. If not, the command fails to be executed.
   - The system checks whether the file contains empty lines. If so, the command fails to be executed.
   - The system checks whether the same configuration exists. If so, the system displays a message indicating that the same configuration exists, and the command is executed successfully.
2. After the file validity is checked, the system reads the file content by line, loads the file content to the memory, and checks the file content:
   - If there is a password that contains more than 128 characters in the file, the command fails to be executed.
   - If the file contains more than 1000 lines, the command fails to be executed.
   - If there are empty lines in the file, the command fails to be executed.
3. After the command is executed successfully, pay attention to the following points:
   - For protection purposes, the file specified by *filename* cannot be modified or deleted.
   - If a slave main control board is installed, the weak password dictionary file is backed up to the slave main control board. For protection purposes, the file cannot be modified or deleted.

Example

Load the weak password dictionary file named **pass1.txt**.

```
<HUAWEI> system-view
[HUAWEI] load security weak-password-dictionary pass1.txt
Info: Success to import the weak password dictionary. The weak password number is 6.
```

13.1.80 navigator first-login enable

Function

The **navigator first-login enable** command enables the browser to display the user registration page during the first login of a web user or enables the system to prompt the creation of a user during the first login of a console port user.

Format

navigator first-login enable

Parameters

None

Views

System view

Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no local user is created on the device. Therefore, the factory configuration file of the device contains the **navigator first-login enable** command. When a user logs in to the device through the web system for the first time, the browser displays the user creation page. After a user is created, the browser does not display the user creation page when the user logs in to the device again through the web system.

In addition, after a user logs in to the device through the console port, the browser does not display the user creation page but displays the user login page, when the user logs in to the device through the web system for the first time. Therefore, if you need to log in to the device through the web system, create a local user for web-based login during a login through the console port.

The factory configuration file of the device contains the **navigator first-login enable** command, removing the need to manually configure this command. The **navigator first-login enable** command can be delivered only through the configuration file, cannot be entered or executed on the device, and is not recorded in buildrun information.

Precautions

When you create an administrator in the factory settings of the device, the creation fails if the specification is reached. In this case, you need to modify the factory configuration file to reserve the specification.

13.1.81 outbound recording-scheme

Function

The **outbound recording-scheme** command applies a policy to a recording scheme to record the connection information.

The **undo outbound recording-scheme** command deletes a policy from a recording scheme. Connection information is not recorded then.

By default, connection information is not recorded.

Format

outbound recording-scheme *recording-scheme-name*

undo outbound recording-scheme

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Incorrect connections may result in network faults, for example, loops. The connection information recorded on a server helps you monitor devices. When network faults occur, you can locate faults based on the connection information recorded on the server.

Prerequisites

A recording scheme has been created using the **recording-scheme** command in the AAA view and an HWTACACS server template has been associated with a recording scheme using the **recording-mode hwtacacs** command in the recording scheme view.

Example

Apply a policy to the recording scheme **scheme** to record the connection information.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template hw1
[HUAWEI-hwtacacs-hw1] quit
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme
[HUAWEI-aaa-recording-scheme] recording-mode hwtacacs hw1
[HUAWEI-aaa-recording-scheme] quit
[HUAWEI-aaa] outbound recording-scheme scheme
```


13.1.82 password alert before-expire

Function

The **password alert before-expire** command sets the number of days in advance users are notified that their passwords are about to expire.

The **undo password alert before-expire** command restores the default number of days in advance users are notified that their passwords are about to expire.

By default, the number of days in advance users are notified that their passwords are about to expire is 30 days. In the factory configuration file, the number of days in advance users are notified that their passwords are about to expire is 0.

Format

password alert before-expire *day*

undo password alert before-expire

Parameters

Parameter	Description	Value
day	Sets the number of days in advance users are notified that their passwords are about to expire. If the value is set to 0, the device does not notify users that their passwords will expire.	The value is an integer that ranges from 0 to 999, in days. The default value is 30 days.

Views

Local administrator password policy view

Default Level

3: Management level

Usage Guidelines

When a user logs in to the device, the device checks how many days the password is valid for. If the number of days is less than the prompt days set in the command, the device notifies the user in how many days the password will expire and asks the user whether to change the password.

- If the user changes the password, the device records the new password and updates the time of password change.
- If the user does not change the password or fails to change the password, the user can still log in as long as the current password is still valid.

Example

Set the number of days in advance users are notified that their passwords are about to expire to 90.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin] password alert before-expire 90
```

13.1.83 password alert original

Function

The **password alert original** command enables the device to prompt users to change initial passwords.

The **undo password alert original** command disables the device from prompting users to change initial passwords.

By default, the device prompts users to change initial passwords.

Format

password alert original

undo password alert original

Parameters

None

Views

Local administrator password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve device security, use this command to enable the initial password change prompt function. When a user logs in to the device:

- If the user enters the initial password, the device displays a message to ask whether to change the initial password. The user can select **Y** or **N**:
  - If the user selects **Y** to change the password, the user needs to enter the old password, new password, and confirm password. The password can be successfully changed only when the old password is correct and the new password and confirm password are the same and meet requirements (password length and complexity). After the password is changed, the user can log in to the device successfully.
  - If the user selects **N** or fails to change the password, the device does not allow the user to log in.

- If the entered password is not the initial password, the device does not display any message and the user can successfully log in.

After the **undo password alert original** command is executed, the initial password alert will be disabled, causing a security risk.

NOTE

The initial password may be the default password, the password created by a local user in the first login, or the password changed by another user (for example, user B changes user A's password, and user A uses the changed password to log in).

Precautions

This function is only valid for Telnet users, HTTP users, SSH users, and terminal users.

Example

Enable the device to prompt users to change initial passwords.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin] password alert original
```

13.1.84 password expire

Function

The **password expire** command sets the password validity period.

The **undo password expire** command restores the default password validity period.

By default, the password validity period is 90 days.In the factory configuration file, the password validity period is 0 days.

Format

password expire *day*

undo password expire

Parameters

Parameter	Description	Value
day	Specifies the password validity period. If the value is 0, the password is permanently valid.	The value is an integer that ranges from 0 to 999, in days. The default value is 90 days.

Views

Local administrator password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve password security, the administrator can use this command to set the validity period for the local user password. When the validity period expires, the password becomes invalid.

If the local user still uses this password to log in to the device, the device allows the user to log in, prompts the user that the password has expired, and asks the user whether to change the password:

- If the user enters Y, the user needs to enter the old password, new password, and confirm password. The password can only be successfully changed when the old password is correct, the new password and confirm password are the same, and the new password meets the password length and complexity requirements. After the password is changed, the user can log in to the device successfully.
- If the user enters N or fails to change the password, the user cannot log in to the device.

Precautions

Changing the system time will affect the password validity status.

After this command is run, the device checks whether the password expires every minute; therefore, there may be a time difference of less than 1 minute.

When the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **local-aaa-user password policy administrato** command to enable the password policy for local administrators.
- Run the **password expire 0** command to configure the passwords of local administrators to be permanently valid.
- Run the **password history record number 0** command to configure the device not to check whether a changed password of a local administrator is the same as any historical password.

Example

Set the password validity period to 120 days.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin] password expire 120
```

13.1.85 password history record number

Function

The **password history record number** command sets the maximum number of historical passwords recorded for each user.

The **undo password history record number** command restores the default maximum number of historical passwords recorded for each user.

By default, a maximum of five historical passwords are recorded for each user. In the factory configuration file, the maximum number of historical passwords recorded for each user is 0.

Format

password history record number *number*

undo password history record number

Parameters

Parameter	Description	Value
number	Specifies the maximum number of historical passwords recorded for each user. If the value is set to 0, the device will not check whether a changed password is the same as any historical password.	The value is an integer that ranges from 0 to 12. The default value is 5.

Views

Local administrator password policy view, local access user password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve password security, it is not recommended that you use a previously used password. You can set the maximum number of historical passwords recorded for each user. When a user changes the password, the device compares the new password against the historical passwords stored on the device. If the new password is the same as a stored password, the device displays an error message to prompt the user that password change fails.

Precautions

When the number of recorded historical passwords reaches the maximum value, the later password will overwrite the earliest password on the device.

After the historical password recording function is disabled, the device does not record historical passwords; however, the passwords that have been stored are retained.

If the **save** command is not run for the historical record of the new user password, the historical record of the new user password is not saved after the device is restarted.

When the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **local-aaa-user password policy administrato** command to enable the password policy for local administrators.
- Run the **password expire 0** command to configure the passwords of local administrators to be permanently valid.
- Run the **password history record number 0** command to configure the device not to check whether a changed password of a local administrator is the same as any historical password.

Example

Set the maximum number of historical passwords recorded for each local administrator to 10.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin] password history record number 10
```

Set the maximum number of historical passwords recorded for each local access user to 10.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy access-user
[HUAWEI-aaa-lupp-acc] password history record number 10
```

13.1.86 permit-domain

Function

The **permit-domain** command specifies permitted domains for WLAN users.

The **undo permit-domain** command deletes the permitted domains of WLAN users.

By default, no permitted domain is specified for WLAN users.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

permit-domain name *domain-name* &<1-4>

undo permit-domain { **name** *domain-name* | **all** }

Parameters

Item	Description	Value
name *domain-name*	Specifies the name of a permitted domain for WLAN users.	The domain must already exist.

Item	Description	Value
all	Deletes the permitted domain for all WLAN users.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a permitted domain is specified on an authentication profile, only the WLAN users in the permitted domain can be authenticated, authorized, or charged.

Prerequisites

Permitted domains have been created using the **domain** command.

Precautions

This command applies only to wireless users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

This command is only available in the NAC unified mode.

Example

Specify permitted domain **dom** for WLAN users to the authentication profile **john**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain dom
[HUAWEI-aaa-domain-dom] quit
[HUAWEI-aaa] quit
[HUAWEI] authentication-profile name john
[HUAWEI-authen-profile-john] permit-domain name dom
```

13.1.87 priority (service scheme view)

Function

The **priority** command configures the

The **undo priority** command restores the default setting.

By default, the user priority is 0.

Format

priority *priority-value*

undo priority

Parameters

Parameter	Description	Value
priority-value	Specifies the user priority.	The value is an integer that ranges from 0 to 1. A larger value indicates a higher priority.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, priorities of all users are the same on a device. As a result, if a large number of common users access an AP in a user-intensive campus office scenarios and the number of users accessed to the AP reaches the upper limit, the subsequent VIP users cannot go online. In this case, you can authorize high priorities for the VIP users using a service scheme to ensure the access success rate of the VIP users. If the number of users accessed to an AP reaches the upper limit and users have been authenticated, the device checks priorities of the users. If the priorities are high, the device forcibly disconnects users with low priorities and allows these users to go online; if the priorities are low, the device does not allow these users to go online.

Precautions

When a CAR configuration for user authorization is delivered by the server or configured in a domain, the CAR configuration does not take effect for VIP users. The following example configures CAR for user authorization in a domain.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name abc
[HUAWEI-qos-abc] car cir 10000 cbs 10240 pbs 10240 inbound //Configure CAR in the QoS profile abc.
[HUAWEI-qos-abc] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] qos-profile abc  //Bind the QoS profile abc to the service scheme test.
[HUAWEI-aaa-service-test] quit
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] service-scheme test   //Bind the service scheme test to the domain test.
```

In a policy association scenario, this function does not take effect on authentication access devices.

Example

Set the user priority in service scheme **s1** to 1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] priority 1
```

13.1.88 recording-mode hwtacacs

Function

The **recording-mode hwtacacs** command associates an HWTACACS server template with a recording scheme.

The **undo recording-mode** command unbinds an HWTACACS server template from a recording scheme.

By default, no HWTACACS server template is associated with a recording scheme.

Format

recording-mode hwtacacs *template-name*

undo recording-mode

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

Recording scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device needs to send the records such as the executed commands, connection information, and system events to the specified HWTACACS accounting server; therefore, an HWTACACS server template needs to be associated with a recording scheme.

Prerequisites

The HWTACACS server template has been created by using the **hwtacacs-server template** command.

Example

Associate the recording scheme **scheme0** with the HWTACACS server template **tacacs1**.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template tacacs1
[HUAWEI-hwtacacs-tacacs1] quit
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme0
[HUAWEI-aaa-recording-scheme0] recording-mode hwtacacs tacacs1
```

13.1.89 recording-scheme

Function

The **recording-scheme** command creates a recording scheme and displays the recording scheme view.

The **undo recording-scheme** command deletes a recording scheme.

By default, no recording scheme is configured on the device.

Format

recording-scheme *recording-scheme-name*

undo recording-scheme *recording-scheme-name*

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a recording scheme takes effect, you can view the records such as the executed commands, connection information, and system-level events on the recording server. The records help you locate network faults. Because a recording scheme needs to be associated with an HWTACACS server template, the recording scheme is configured only when HWTACACS authentication or authorization is performed.

Creating a recording template using the **recording-scheme** command is mandatory for configuration.

Follow-up Procedure

Run the **recording-mode hwtacacs** command to associate an HWTACACS server template with the recording scheme.

After a recording scheme is created and associated with an HWTACACS server template, perform the following configurations in the AAA view:

- Run the **cmd recording-scheme** command to apply a policy in a recording scheme to record the commands executed on the device.
- Run the **outbound recording-scheme** command to apply a policy in a recording scheme to record the connection information.
- Run the **system recording-scheme** command to apply a policy in a recording scheme to record the system events.

Precautions

If the recording scheme to be configured does not exist, the **recording-scheme** command creates a recording scheme and displays the recording scheme view. If the recording scheme to be configured already exists, the **recording-scheme** command displays the recording scheme view.

Before deleting a recording scheme, ensure that the scheme has not been referenced by the **cmd recording-scheme** or **outbound recording-scheme** or **system recording-scheme** command.

Example

Create a recording scheme **scheme0**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme0
[HUAWEI-aaa-recording-scheme0]
```

13.1.90 redirect-acl

Function

The **redirect-acl** command configures the ACL used for redirection in a service scheme.

The **undo redirect-acl** command deletes the ACL used for redirection in a service scheme.

By default, no ACL for redirection is configured in the service scheme.

Format

redirect-acl [**ipv6**] { *acl-number* | **name** *acl-name* }

undo redirect-acl [**ipv6**]

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1, S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S6720-EI, S6735-S, , S6720S-EI support the **ipv6** parameter.

Only wired users support the authorization of the IPv6 ACL used for redirection.

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 ACL used for redirection.	-
acl-number	Specifies the number of the ACL used for redirection.	The value ranges from 3000 to 3999 for wired users and from 3000 to 3031 for wireless users, and it must exist.
name *acl-name*	Specifies the name of the ACL used for redirection.	The ACL name must exist. The length ranges from 1 to 64.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In some authentication scenarios, after users succeed in authentication, the administrator needs to redirect HTTP/HTTPS traffic matching ACL permit rules to the Portal authentication page where users are authenticated again.

Precautions

Before running this command, you are advised to run the **acl** or **acl name** command to create an ACL.

If the ACL is not created before and after this command is run, the redirection ACL will fail to be delivered.

To redirect HTTPS traffic, run the **authentication https-redirect enable** command to configure the HTTPS redirection function.

After the **authentication mode multi-share** command is configured in the authentication profile, authorization redirection ACLs will not be supported.

Example

Configure ACL 3001 for redirection in the service scheme **svcscheme1**.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme svcscheme1
[HUAWEI-aaa-service-svcscheme1] redirect-acl 3001
```

13.1.91 remote-user authen-fail unblock

Function

The **remote-user authen-fail unblock** command unlocks remote AAA authentication accounts.

Format

remote-user authen-fail unblock { **all** | **username** *username* }

Parameters

Parameter	Description	Value
all	Unlocks all accounts that fail the remote AAA authentication.	-
username *username*	Unlocks a specified account that fails the remote AAA authentication.	The value is a string of 1 to 253 case-insensitive characters without spaces.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

You may need to unlock remote AAA authentication accounts in the following situations:

- When a user enters an incorrect user name or password fewer times than the maximum permitted, run the **remote-user authen-fail unblock** command to unlock the user and delete the incorrect record of the user from the device.
- When a user is incorrectly locked or needs to be unlocked due to special reasons, run the **remote-user authen-fail unblock** command to unlock the user.

Example

Unlock the remote AAA authentication account **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] remote-user authen-fail unblock username test
```

13.1.92 reset aaa

Function

Using the **reset aaa** command, you can clear records of abnormal offline, user offline and failure to get online.

Format

reset aaa { **abnormal-offline-record** | **offline-record** | **online-fail-record** }

Parameters

Parameter	Description	Value
abnormal-offline-record	Clears records of user abnormal offline.	-
offline-record	Clears records of user offline.	-
online-fail-record	Clears records of user failure to get online.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command allows you to clear records of user offline, abnormal offline, and failure to get online. After the records are cleared, the function of recording information is enabled.

Example

Clear user offline records.

```
<HUAWEI> system-view
[HUAWEI] reset aaa offline-record
```

13.1.93 reset aaa statistics offline-reason

Function

Using the **reset aaa statistics offline-reason** command, you can clear the statistics about reasons why users go offline.

Format

reset aaa statistics offline-reason

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **reset aaa statistics offline-reason** command to delete the statistics about reasons why users go offline, and then collect new statistics.

Example

Clear the statistics about reasons why users go offline.

```
<HUAWEI> reset aaa statistics offline-reason
```

13.1.94 reset access-user statistics

Function

The **reset access-user statistics** command deletes the statistics on access user authentication.

Format

reset access-user statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When diagnosing and locating faults related to access user authentication, you need to collect statistics on user login and logout information within a period of time. Before the statistics collection, you can run the **reset access-user statistics** command to clear the historical statistics, and then run the **display access-user statistics** command to view the current statistics.

Example

Delete the statistics on access user authentication.

```
<HUAWEI> reset access-user statistics
Info: Successful to reset access-user statistics.
```

13.1.95 reset local-user password history record

Function

The **reset local-user password history record** command clears historical passwords stored for the local user.

Format

reset local-user [*user-name*] **password history record**

Parameters

Parameter	Description	Value
user-name	Clears the historical passwords of the specified user. If this parameter is not specified, the historical passwords of all local users are cleared.	The local user must exist on the device.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the administrator wants to record historical passwords of local users again, this command can be used to clear existing historical passwords.

Precautions

After this command is used, all historical passwords on the device are deleted and cannot be restored. This operation has security risks, so exercise caution when using it.

Example

Clear historical passwords of all local users.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] reset local-user password history record
Warning: Clear history password records, there is a security risk. Continue?[Y/N] y
```

13.1.96 server no-response accounting

Function

The **server no-response accounting** command configures a device to continue sending accounting packets when the accounting function is configured and a user is authenticated using the local authentication mode after the server does not respond to the user's authentication request.

The **undo server no-response accounting** command restores the default setting.

By default, when the accounting function is configured, the device does not send accounting packets when the server does not respond to a user's authentication request and the user then is authenticated using local authentication.

Format

server no-response accounting

undo server no-response accounting

Parameters

None

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Typically, a server functions as both the remote accounting server and the authentication server. If the authentication server does not respond, the accounting server also does not respond. When accounting and authentication + local authentication are configured on a device, a user is authenticated using the local authentication mode after the server does not respond to the user's authentication request. Because the accounting server also does not respond, after the user is authenticated using the local authentication mode, the device still sends accounting packets. As a result, the user goes offline because of accounting-start failures. To prevent this issue, the device does not send accounting packets by default when a user is authenticated using the local authentication mode after the server does not respond to the user's authentication request.

Example

Configure a device not to send accounting packets when the accounting function is configured and a user is authenticated using the local authentication mode after the server does not respond to the user's authentication request.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme authen1
[HUAWEI-aaa-authen-authen1] authentication-mode radius local
[HUAWEI-aaa-authen-authen1] undo server no-response accounting
[HUAWEI-aaa-authen-authen1] quit
[HUAWEI-aaa] accounting-scheme acc1
[HUAWEI-aaa-accounting-acc1] accounting-mode radius
```

13.1.97 server no-response authorization

Function

The **server no-response authorization** command configures the device to perform authorization in the configured authorization sequence after local authentication is used when the server does not respond to users' authentication requests and both server authentication and local authentication are configured.

The **undo server no-response authorization** command configures the device to request local authorization after local authentication is used when the server does not respond to users' authentication requests and both server authentication and local authentication are configured.

By default, when both server authentication and local authentication are configured, the device requests local authorization after local authentication is used when the server does not respond to users' authentication requests.

Format

server no-response authorization

undo server no-response authorization

Parameters

None

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

In most cases, if both remote authentication and local authentication are configured on a device and remote authentication does not respond, the device selects local authentication. After local authentication is performed on a user, the device requests local authorization. After the **server no-response authorization** command is run, the device still uses the configured authorization mode.

Precautions

RADIUS authentication and authorization are integrated. Therefore, when RADIUS authentication and local authentication are configured, if remote authentication does not respond, remote authorization does not respond, and the device still uses local authorization.

You can run the **display access-user user-id** command to check the authentication mode and authorization mode after this command is configured.

Example

When HWTACACS+local authentication and authorization are configured, the device requests authorization in the configured authorization mode instead of requesting local authorization after local authentication is used if the server does not respond.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme authen1
[HUAWEI-aaa-authen-authen1] authentication-mode hwtacacs local
[HUAWEI-aaa-authen-authen1] server no-response authorization
[HUAWEI-aaa-authen-authen1] quit
```

13.1.98 security-name enable

Function

The **security-name enable** command enables the security string function.

The **undo security-name enable** command disables the security string function.

By default, the security string function is enabled.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

security-name enable

undo security-name enable

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Some special clients use user names in the format of **username@domain*securitystring** in which a security string and a security string delimiter (*) are added to the user name. To ensure that the AAA server can identify such user names, run the **security-name enable** command to enable the security string function on the device. When sending a user name to the AAA server, the device deletes ***securitystring** and only uses **username@domain** for authentication.

You can run the **security-name-delimiter** command to modify the security string delimiter.

Example

Enable the security string function.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] security-name enable
```

13.1.99 security-name-delimiter

Function

The **security-name-delimiter** command configures a delimiter for a security string.

The **undo security-name-delimiter** command restores the default delimiter for a security string.

By default, the delimiter for a security string in the AAA view is *, and no delimiter is available in the authentication profile view.

NOTE

This command only applies to 802.1X users. If CHAP or PAP authentication is configured for 802.1X users, the device removes the security string, but does not encapsulate it into the HW-SecurityStr attribute. If EAP authentication is configured for 802.1X users, the device removes the security string and encapsulates it into the HW-SecurityStr attribute.

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

security-name-delimiter *delimiter*

undo security-name-delimiter

Parameters

Parameter	Description	Value
delimiter	Specifies a delimiter for a security string.	The value is of the enumerated type. The value can be \ / : < > | @ ' % or *.

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

Some STAs may use the user name in the format of **username@domain*securitystring**. * is the security string delimiter. To enable the AAA server to identify this type of user name, you need to configure a delimiter for a security string on the device. In this way, when sending the user name to the AAA server, the device deletes ***securitystring** and only uses **username@domain** for authentication.

If the server needs to identify a security string, for example *, you need to configure other security string delimiters except *. For example, if a client is configured with a user name in the format of **username@domain*securitystring**, the device needs to be configured with other security string delimiters except *. In this way, when sending the user name to the server, the device still uses the user name in the format of **username@domain*securitystring** for authentication.

Precautions

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the authentication profile, the

configuration takes effect for only the users connected to this authentication profile.

The delimiter for a security string cannot be the same as the domain name delimiter.

If you run the **security-name-delimiter** command in the AAA view, the delimiter for a security string is configured globally.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

Example

Configure the delimiter for a security string as / in the AAA view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] security-name-delimiter /
```

13.1.100 service-scheme (aaa domain view)

Function

The **service-scheme** command applies a service scheme to a domain.

The **undo service-scheme** command unbinds a service scheme from a domain.

By default, no service scheme is bound to a domain.

Format

service-scheme *service-scheme-name*

undo service-scheme

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme.	The value must be an existing service scheme name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The authorization configuration in a service scheme takes effect only when the service scheme is applied to a domain.

Prerequisites

A service scheme has been created and configured with required parameters.

Example

Apply the service scheme **srvscheme1** to the domain **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme srvscheme1
[HUAWEI-aaa-service-srvscheme1] quit
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] service-scheme srvscheme1
```

13.1.101 service-scheme (AAA view)

Function

The **service-scheme** command creates a service scheme and displays the service scheme view.

The **undo service-scheme** command deletes a service scheme.

By default, no service scheme is configured.

Format

service-scheme *service-scheme-name*

undo service-scheme *service-scheme-name*

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: /, \, :, *, ?, '', <, >, |, @, ', and %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The service scheme is used to assign IP address pool and DNS server parameters to users.

Follow-up Procedure

Run the **service-scheme (AAA domain view)** command to apply the service scheme to a domain.

Precautions

In traditional NAC mode, the authorization scheme is not supported.

If the service scheme to be configured does not exist, the **service-scheme (AAA view)** command creates a service scheme and displays the service scheme view. If the service scheme to be configured already exists, the **service-scheme (AAA view)** command displays the service scheme view.

To delete or modify the service scheme applied to a domain, run the **undo service-scheme (AAA domain view)** command to unbind the service scheme from the domain.

Example

Create a service scheme **srvscheme1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme srvscheme1
[HUAWEI-aaa-service-srvscheme1]
```

13.1.102 state (AAA domain view)

Function

The **state** command configures the state of a domain.

The **undo state** command restores the state of a domain.

By default, a domain is in active state after being created.

Format

state { **active** | **block** [**time-range** *time-name* &<1-4>] }

undo state [**block time-range** [*time-name* &<1-4>]]

Parameters

Parameter	Description	Value
active	Sets the domain state to active.	-

Parameter	Description	Value
block	Sets the domain state to blocking.	-
time-range *time-name*	Indicates the block time range of the domain. *time-name* specifies the name of the block time range. If this parameter is not specified, the domain is always blocked.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word **all** cannot be specified as a time range name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If exceptions occur during service configuration, set the domain in blocking state to block access of new users. After the service configuration is complete, set the domain in active state.

Prerequisite

Before specifying the *time-name* parameter, ensure that the time range has been created using the **time-range** command.

Precautions

After the **state block** command is run to set the domain state to block, online users in the domain are not affected.

After the **state block time-range** command is run to set the state of a domain including online users to block, the domain state turns from active to block within the specified time range, and online users are forced to go offline.

Example

Set the state of the domain **vipdomain** to blocking.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain vipdomain
[HUAWEI-aaa-domain-vipdomain] state block
```

Set the name of the time range in which the **vipdomain** domain state turns to block to **tim**.


```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain vipdomain
[HUAWEI-aaa-domain-vipdomain] state block time-range tim
Warning: This operation may cause online users to go offline. Continue? [Y/N]Y
```

13.1.103 statistic enable (AAA domain view)

Function

The **statistic enable** command enables traffic statistics collection for domain users.

The **undo statistic enable** command disables traffic statistics collection for domain users.

By default, traffic statistics collection is disabled for domain users.

NOTE

After the **statistic enable** command is executed, statistics about both IPv4 and IPv6 upstream and downstream traffic will be collected. After the **accounting dual-stack separate** command is executed, IPv4 and IPv6 traffic statistics will be collected separately. The following describes the traffic statistics function.

- On the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, statistics about both IPv4 and IPv6 upstream and downstream traffic can be collected only when the user access mode is the **multi-share** mode.
- On the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, after an authentication profile in which the user access mode is set to **multi-share** is applied to an Eth-Trunk interface, the device does not support the collection of statistics about both IPv4 and IPv6 upstream and downstream traffic for the users bound to the authentication profile.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, after an authentication profile in which the user access mode is set to **multi-share** is applied to an Eth-Trunk interface, the device does not support the collection of statistics about both IPv4 and IPv6 upstream and downstream traffic for the users bound to the authentication profile.
- In a single-MAC multi-IP scenario, only IPv4 traffic statistics can be collected.
- The device does not support Layer 3 IPv6 Portal authentication or traffic statistics collection of Layer 3 IPv6 Portal authentication users.
- If a device does not support Layer 2 IPv6 Portal authentication, the device can collect statistics about IPv4 and IPv6 upstream and downstream traffic after Portal authentication is triggered for IPv4 users. The following devices do not support Layer 2 IPv6 Portal authentication: S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S.

Format

statistic enable

undo statistic enable

Parameters

None

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To implement traffic-based accounting, you can use this command to enable traffic statistics collection for a domain. Then the device collects traffic statistics for the users in the domain. If an accounting server is configured, the device sends traffic statistics to the accounting server through accounting packets so that the server performs accounting for the users based on traffic statistics.

Follow-up Procedure

Run the **display access-user** command to view traffic statistics of users.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

For the S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, if users are authorized with CAR during the configuration of traffic statistics collection, only CAR takes effect, and traffic statistics collection does not take effect.

This command collects service statistics for domain users. The device sends the statistics to the accounting server.

On the S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI:

- Traffic statistics are collected based on interfaces.
- The traffic statistics collection is valid for domain users only when interfaces are physical interface and each interface connects to only one domain user.
- The interface traffic statistics for the first 15s when a user goes online are not collected.
- When users are online, you cannot run the **reset_counters_interface** command to clear interface traffic statistics. Otherwise, the user traffic statistics are inaccurate.

Example

Enable traffic statistics collection for domain users.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] statistic enable
```


13.1.104 system recording-scheme

Function

The **system recording-scheme** command applies a policy in a recording scheme to record the system events.

The **undo system recording-scheme** command deletes a policy from a recording scheme. System events are not recorded then.

By default, system events are not recorded.

Format

system recording-scheme *recording-scheme-name*

undo system recording-scheme

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system events recorded on an HWTACACS server help you monitor devices. When network faults occur, you can isolate faults based on the system events recorded on the HWTACACS server.

Prerequisites

A recording scheme has been created using the **recording-scheme** command in the AAA view and an HWTACACS server template has been associated with a recording scheme using the **recording-mode hwtacacs** command in the recording scheme view.

Precautions

Currently, the device can record only the events caused by the **reboot** command.

Example

Apply a policy in the recording scheme **scheme** to record the system events.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template hw1
[HUAWEI-hwtacacs-hw1] quit
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme
[HUAWEI-aaa-recording-scheme] recording-mode hwtacacs hw1
[HUAWEI-aaa-recording-scheme] quit
[HUAWEI-aaa] system recording-scheme scheme
```

13.1.105 unload security weak-password-dictionary

Function

The **unload security weak-password-dictionary** command uninstalls a weak password dictionary.

Format

unload security weak-password-dictionary

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Run this command to uninstall the weak password dictionary from the system.

Example

Unload a weak password dictionary.

```
<HUAWEI> system-view
[HUAWEI] unload security weak-password-dictionary
```

13.1.106 user-group (AAA domain view)

Function

The **user-group** command binds the users in a domain to the authorization information of a user group.

The **undo user-group** command unbinds the users in a domain from the authorization information of a user group.

By default, no authorization information of a user group is bound to the users in a domain.

NOTE

This command is supported only in the NAC common mode.

Format

user-group *group-name*

undo user-group

Parameters

Parameter	Description	Value
group-name	Specifies the name of a user group.	The user group name must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **user-group** command in the AAA domain to bind the users in a domain to the authorization information of a user group.

Precautions

- The user group to be specified using the **local-user user-group** command must have been created using the **user-group** command.
- A user group cannot be deleted after being referenced to a domain using this command.
- Huawei proprietary attribute 82 delivered by RADIUS cannot be used together with the function of binding authentication information of a user group to a domain.
- The priority of the authorization information delivered using this command is lower than that of the authorization information delivered using the **portal free-rule** *rule-id* **source ip** *ip-address* **mask** { *mask-length* | *ip-mask* } [**mac** *mac-address*] [**interface** *interface-type interface-number*] **destination user-group** *group-name* command.

Example

Bind the user group **group1** to the domain **test**.


```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] user-group group1
```

13.1.107 user-password complexity-check

Function

The **user-password complexity-check** command enables password complexity check.

The **undo user-password complexity-check** command disables password complexity check.

By default, password complexity check is enabled on a device. A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.

Format

user-password complexity-check [**three-of-kinds** | enhance]

undo user-password complexity-check

Parameters

Parameter	Description	Value
three-of-kinds	Indicates that a password must contain at least three of the following: uppercase letters, lowercase letters, digits, and special characters.	-
enhance	Indicates enhanced password complexity check. A password must contain at least eight characters, including at least three of the following: digits, lowercase letters, uppercase letters, and special characters. The password and user name cannot contain each other (regardless of the case). Otherwise, the password cannot pass the complexity check.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the versions earlier than V200R003, the device uses simple user name and password rules, so the user names and passwords are easy to manage and remember; however, weak passwords have security risks. In V200R003 and later versions, the device poses stricter requirements on user names and passwords. After you create a local user using the **local-user** command, the password must pass a complexity check performed by the device.

You can choose whether to enable password complexity check in V200R005 and later versions.

Precautions

To ensure device security, ensure that password complexity check is enabled and change the password periodically.

Example

Disable password complexity check.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] undo user-password complexity-check
```

13.1.108 vlan block-time

Function

The **vlan block-time** command sets the lockout time of VLANs in a VLAN pool.

The **undo vlan block-time** command restores the default lockout time of VLANs in a VLAN pool.

By default, the lockout time of VLANs in a VLAN pool is 30 minutes.

Format

vlan block-time *block-time*

undo vlan block-time

Parameters

Parameter	Description	Value
block-time	Specifies the lockout time of VLANs.	The value is an integer in the range of 5 to 1440, in minutes.

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the VLAN assignment algorithm in a VLAN pool is set to **hash** and the **dhcp update vlan assignment** command has been run to enable the function of reassigning VLANs in the VLAN pool, a VLAN will be locked for 30 minutes by default and cannot be assigned to users after all IP addresses in the VLAN have been assigned. To adjust the lockout time of VLANs in the VLAN pool, run the **vlan block-time** command.

Prerequisites

The VLAN assignment algorithm has been set to **hash** using the **assignment hash** command.

Precautions

The **vlan block-time** command takes effect after the **dhcp update vlan assignment** command is run to enable the function of reassigning VLANs in the VLAN pool.

After the **assignment even** command is run, the **assignment hash** command configuration will be cleared. Exercise caution when running the **assignment even** command.

This function takes effect only for wired users.

Authentication access devices in the policy association scenario do not support this function.

Example

Set the lockout time of VLANs in a VLAN pool to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] assignment hash
[HUAWEI-vlan-pool-test] dhcp update vlan assignment
[HUAWEI-vlan-pool-test] vlan block-time 5
```

13.1.109 vlan pool

Function

The **vlan pool** command creates a VLAN pool and displays the VLAN pool view, or displays the view of an existing VLAN pool.

The **undo vlan pool** command deletes a VLAN pool.

By default, no VLAN pool is created on a device.

Format

vlan pool *pool-name*

undo vlan pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Specifies the name of a VLAN pool.	The value is a string of 1 to 31 characters. It cannot contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ")

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VLAN pool is a combination of multiple VLANs and is used to simplify network deployment. The administrator plans the VLANs of users in a department as a VLAN pool. After a user passes the authentication, the authentication server authorizes the VLAN pool to the user. The device allocates VLANs in the VLAN pool to users based on the VLAN assignment algorithm. In this way, VLANs can be planned for multiple departments without the need of calculating the number of users of each department.

On a WLAN, the access modes and access locations of wireless users are flexible. Users often connect to the same WLAN at a site such as the office entrance or stadium entrance, and then roam to WLANs covered by other APs. If each SSID has only one service VLAN to deliver wireless access to wireless users, IP address resources may become insufficient in areas where many wireless users access the WLAN, and IP addresses in the other areas are wasted. The VLAN pool can be configured as the service VLAN for wireless users so that one SSID can support multiple service VLANs simultaneously. New users are dynamically assigned to VLANs in the VLAN pool, which reduces the number of users in each VLAN and also the size of the broadcast domain. Additionally, IP addresses are evenly allocated, preventing IP address waste.

Follow-up Procedure

1. Run the **vlan** command to add VLANs to the VLAN pool.
2. Set the standard RADIUS attribute **Tunnel-Private-Group-ID** assigned to users who pass authentication by the RADIUS server so that wired users can be added to the specified VLAN pool.
3. For wireless users, three methods are available to apply a VLAN pool:
   - Run the **vap-profile** *profile-name* **wlan** *wlan-id* **radio** { *radio-id* | **all** } **service-vlan vlan-pool** *pool-name* command to configure the specified VLAN pool as the service VLAN of wireless users in the specified VAP profile.

- Run the **service-vlan vlan-pool** *pool-name* command in the VAP profile view to configure the VLAN pool as the service VLAN of wireless users in the VAP profile.
- On the RADIUS server, configure the standard RADIUS attribute **Tunnel-Private-Group-ID** for authenticated users to add the users to the specified VLAN pool.

Precautions

- After a VLAN pool is configured as a service VLAN for wireless users, the VLAN pool cannot be configured as the VLAN pool assigned to users who pass authentication by the RADIUS server.
- After a VLAN pool is configured as a service VLAN for wireless users, VLANs in the VLAN pool cannot be deleted. To delete the VLAN pool, cancel the service VLAN configuration of the VLAN pool.
- If a VLAN or the VLAN pool to which a VLAN belongs has been configured as a service VLAN for the WLAN network, the VLAN cannot be configured as a super-VLAN. Similarly, if a VLAN has been configured as a super-VLAN, the VLAN or the VLAN pool to which the VLAN belongs cannot be configured as a service VLAN for the WLAN network. In addition, if a VLAN pool has been configured as a service VLAN for a WLAN network, a super-VLAN cannot be added to the VLAN pool.
- In scenarios where a dual-stack address pool is configured, a user successfully obtains an IP address if the VLAN pool has assigned an IPv4 or IPv6 address to it. In this case, the VLAN pool will not assign a new VLAN to this user.

Example

Create the VLAN pool **test** and display the VLAN pool view.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test]
```

13.1.110 vlan (VLAN pool view)

Function

The **vlan** command adds VLANs to a VLAN pool.

The **undo vlan** command deletes VLANs from a VLAN pool.

By default, no VLAN is available in a VLAN pool.

Format

vlan { *start-vlan* [**to** *end-vlan*] } &<1-10> [**max-user** *number*]

undo vlan { { *start-vlan* [**to** *end-vlan*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
start-vlan [**to** *end-vlan*]	Specifies the range of VLAN IDs. *start-vlan* and *end-vlan* determine a VLAN range. *start-vlan* must be equal to or smaller than *end-vlan*.	The value is an integer in the range from 1 to 4094.
max-user *number*	Specifies the maximum number of users in a VLAN.	The value is an integer, varies according to the device model.

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VLAN pool is a combination of multiple VLANs. It is used to simplify network deployment. To add specified VLANs to a VLAN pool, run the **vlan (VLAN pool view)** command.

If the VLAN assignment algorithm of a VLAN pool is **hash**, you can specify **max-user** *number* to set the maximum number of users allowed in a specific VLAN based on the number of IP addresses in the IP address pool on the DHCP server. When the number of online users in the VLAN reaches the upper limit, users will not go online through the VLAN. This ensures that all online users can obtain IP addresses.

Precautions

- A maximum of 128 VLANs can be added to a VLAN pool.
- Deleting a VLAN will interrupt services of users using the VLAN. Exercise caution when you perform this operation.
- A nonexistent VLAN can also be added to a VLAN pool. However, you need to create the VLAN after adding a nonexistent VLAN to a VLAN pool; otherwise, the VLAN does not take effect.
- The VLAN reserved for a stack cannot be added to a VLAN pool.
- **max-user** *number* is valid only for users authorized a VLAN pool and takes effect only when the VLAN assignment algorithm of a VLAN pool is **hash**.

Example

Add VLANs 9, 12, 13, and 14 to the VLAN pool **test**.


```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] vlan 9 12 to 14
```

13.2 RADIUS Configuration Commands

13.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.2.2 accounting-copy radius-server

Function

The **accounting-copy radius-server** command enables the RADIUS accounting packet copy function and configures a RADIUS server template for level-2 accounting.

The **undo accounting-copy radius-server** command disables the RADIUS accounting packet copy function.

By default, the RADIUS accounting packet copy function is disabled.

Format

accounting-copy radius-server *template-name*

undo accounting-copy radius-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of a RADIUS server template.	The RADIUS server template must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The existing RADIUS server on the network performs authentication, authorization, and accounting for users. User login and logout information is sent to the server through accounting packets. Users want to deploy an independent RADIUS accounting server (called the level-2 RADIUS accounting server) to obtain user login and logout information for analyzing user behavior and managing users' access to the network. However, the device currently does not send accounting packets to the level-2 RADIUS accounting server. In this case, you can configure the RADIUS accounting packet copy function on the device. After this function is configured, the device sends user login and logout information to the level-2 RADIUS accounting server through accounting packets for third-party user behavior analysis.

Prerequisites

The RADIUS server template has been created using the **radius-server template** command.

Precautions

- Ensure that the IP address of the configured level-2 RADIUS accounting server is different from that of the level-1 RADIUS accounting server (including the active/standby RADIUS accounting server).
- Ensure that the level-2 RADIUS accounting server template configured in the domain is different from the RADIUS server template for authentication and accounting in the domain. If they are the same, the accounting-copy radius-server command cannot be configured and the system displays an error message during the command configuration.

Example

In the **test** domain, set the IP addresses of the RADIUS authentication and accounting servers to 10.1.1.1, their port numbers to 1813 and 1814, respectively, and RADIUS server template to **t1**. Set the IP address and port number of the RADIUS server for level-2 accounting to 10.1.1.2 and 1814, respectively, and the RADIUS server template to **t2**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template t1
[HUAWEI-radius-t1] radius-server authentication 10.1.1.1 1813
[HUAWEI-radius-t1] radius-server accounting 10.1.1.1 1814
[HUAWEI-radius-t1] quit
[HUAWEI] radius-server template t2
[HUAWEI-radius-t2] radius-server accounting 10.1.1.2 1814
[HUAWEI-radius-t2] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] radius-server t1
[HUAWEI-aaa-domain-test] accounting-copy radius-server t2
```

13.2.3 called-station-id mac-format

Function

The **called-station-id mac-format** command sets the encapsulation format of the MAC address in the called-station-id (Type 30) attribute of RADIUS packets.

The **undo called-station-id mac-format** command restores the default encapsulation format of the MAC address in the called-station-id attribute of RADIUS packets.

By default, the encapsulation format of the MAC address in the called-station-id attribute of RADIUS packets is XX-XX-XX-XX-XX-XX, in uppercase.

Format

called-station-id mac-format { **dot-split** | **hyphen-split** | **colon-split**} [**mode1** | **mode2**] [**lowercase** | **uppercase**]

called-station-id mac-format unformatted [**lowercase** | **uppercase**]

undo called-station-id mac-format

Parameters

Parameter	Description	Value
dot-split	Indicates that the dot (.) is used as the separator in a MAC address.	-
hyphen-split	Indicates that the hyphen (-) is used as the separator in a MAC address.	-
colon-split	Indicates that the colon (:) is used as the separator in a MAC address.	-
unformatted	Indicates that no separator is used in a MAC address.	-
mode1	Indicates that the MAC address in the calling-station-id attribute uses the XXXX-XXXX-XXXX, XXXX:XXXX:XXXX, or XXXX.XXXX.XXXX format.	-
mode2	Indicates that the MAC address in the calling-station-id attribute uses the XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, or XX.XX.XX.XX.XX.XX format.	-
lowercase	Indicates that the MAC address in the called-station-id attribute uses the lowercase.	-
uppercase	Indicates that the MAC address in the called-station-id attribute uses the uppercase.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The Called-station-id (Type 30) attribute indicates the MAC address and SSID of an AP. The default format of the MAC address in the called-station-id attribute of RADIUS packets from the device is XX-XX-XX-XX-XX-XX. If the RADIUS server does not support the default format, run the **called-station-id mac-format** command to change the format.

Example

Set the dot as the separator in a MAC address and the encapsulation format of the MAC address in the called-station-id attribute to XX.XX.XX.XX.XX.XX in uppercase.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] called-station-id mac-format dot-split mode2 uppercase
```

13.2.4 called-station-id wlan-user-format

Function

The **called-station-id wlan-user-format** command sets the encapsulation content of the Called-station-id (30) attribute in RADIUS packets.

The **undo called-station-id wlan-user-format** command restores the default encapsulation content of the Called-station-id (30) attribute in RADIUS packets.

By default, the encapsulation content of the Called-station-id (30) attribute is the AP's MAC address and SSID separated with a colon (:), in the format of ap-mac:ssid.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this function.

Format

called-station-id wlan-user-format { **ap-mac** | **ac-mac** | **ac-ip** | **ap-name** | **ap-group-name** | **vlanid** | **ap-location** } [**include-ssid** [**delimiter** *delimiter*]]

undo called-station-id wlan-user-format

Parameters

Parameter	Description	Value
ap-mac	Indicates that the encapsulation content of the Called-station-id (30) attribute is the AP's MAC address.	-

Parameter	Description	Value
ac-mac	Indicates that the encapsulation content of the Called-station-id (30) attribute is the AC's MAC address.	-
ac-ip	Indicates that the encapsulation content of the Called-station-id (30) attribute is the AC's IP address.	-
ap-name	Indicates that the encapsulation content of the Called-station-id (30) attribute is the AP name.	-
ap-group-name	Indicates that the encapsulation content of the Called-station-id (30) attribute is the name of the AP group to which the AP belongs.	-
vlanid	Indicates that the encapsulation content of the Called-station-id (30) attribute is the outer VLAN through which the user goes online.	-
ap-location	Indicates that the encapsulation content of the Called-station-id (30) attribute is location information of the AP.	-
include-ssid	Indicates that the encapsulation content of the Called-station-id (30) attribute contains the SSID. If this parameter is not specified, the encapsulation content of the Called-station-id (30) attribute does not contain the SSID.	-
delimiter *delimiter*	Specifies the delimiter before the SSID when the encapsulation content of the Called-station-id (30) attribute contains the SSID.	The value is of enumerated type. The value can be \ / : < > | @ ' % * + - & ! # ^ or ~. The default value is :.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The Called-station-id (30) attribute indicates the number of the NAS. For wireless users, the default encapsulation content of this attribute is the AP's MAC address and SSID, in the format of ap-mac:ssid. You can run the **called-station-id wlan-user-format** command to modify the encapsulation content of this attribute based on the format of this attribute supported by the RADIUS server.

You can run the **called-station-id mac-format** command to set the encapsulation format of the MAC address of the AP or AC.

Example

Set the encapsulation content of the Called-station-id (30) attribute in RADIUS packets to the AC's MAC address without the SSID.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] called-station-id wlan-user-format ac-mac
```

13.2.5 calling-station-id mac-format

Function

The **calling-station-id mac-format** command sets the encapsulation format of the MAC address in the calling-station-id (Type 31) attribute of RADIUS packets.

The **undo calling-station-id mac-format** command restores the default encapsulation format of the MAC address in the calling-station-id attribute of RADIUS packets.

By default, the encapsulation format of the MAC address in the calling-station-id attribute of RADIUS packets is xxxx-xxxx-xxxx, in lowercase.

Format

calling-station-id mac-format { **dot-split** | **hyphen-split** | **colon-split** } [**mode1** | **mode2**] [**lowercase** | **uppercase**]

calling-station-id mac-format unformatted [**lowercase** | **uppercase**]

calling-station-id mac-format bin

undo calling-station-id mac-format

Parameters

Parameter	Description	Value
dot-split	Indicates that the dot (.) is used as the separator in a MAC address.	-
hyphen-split	Indicates that the hyphen (-) is used as the separator in a MAC address.	-
colon-split	Indicates that the colon (:) is used as the separator in a MAC address.	-
unformatted	Indicates that no separator is used in a MAC address.	-
mode1	Indicates that the MAC address in the calling-station-id attribute uses the XXXX-XXXX-XXXX, XXXX:XXXX:XXXX, or XXXX.XXXX.XXXX format.	-
mode2	Indicates that the MAC address in the calling-station-id attribute uses the XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, or XX.XX.XX.XX.XX.XX format.	-
lowercase	Indicates that the MAC address in the calling-station-id attribute uses the lowercase.	-
uppercase	Indicates that the MAC address in the calling-station-id attribute uses the uppercase.	-
bin	Indicates that the MAC address in the calling-station-id attribute uses the binary form.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The default format of the MAC address in the calling-station-id (Type 31) attribute of RADIUS packets from the device is xxxx-xxxx-xxxx. If the RADIUS server does not support the default format, run the **calling-station-id mac-format** command to change the format.

Example

Set the dot as the separator in a MAC address and the encapsulation format of the MAC address in the calling-station-id attribute to XX.XX.XX.XX.XX.XX in uppercase.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] calling-station-id mac-format dot-split mode2 uppercase
```

13.2.6 display radius-attribute

Function

The **display radius-attribute** command displays the RADIUS attributes supported by the device.

Format

display radius-attribute [**name** *attribute-name* | **type** { *attribute-number1* | **huawei** *attribute-number2* | **microsoft** *attribute-number3* | **dslforum** *attribute-number4* }]

Parameters

Parameter	Description	Value
name *attribute-name*	Displays a specified RADIUS attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
type { *attribute-number1* | **huawei** *attribute-number2* | **microsoft** *attribute-number3* | **dslforum** *attribute-number4* }	Displays the RADIUS attribute of a specified type: • *attribute-number1* specifies the standard attribute. • **huawei** *attribute-number2* specifies a Huawei attribute. • **microsoft** *attribute-number3* specifies a Microsoft attribute. • **dslforum** *attribute-number4* specifies a Digital Subscriber Line Forum attribute.	The value of *attribute-number1*, *attribute-number2*, *attribute-number3*, or *attribute-number4* is an integer that ranges from 1 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before connecting the device to a RADIUS server, run the **display radius-attribute** command to view the RADIUS attributes supported by the device. If the device and RADIUS server support different RADIUS attributes according to the command output, run the **radius-attribute disable** command on the device to disable RADIUS attributes that are not supported by the RADIUS server or run the **radius-attribute translate** command to translate RADIUS attributes.

Example

Display the RADIUS attributes supported by the device.

```
<HUAWEI> display radius-attribute
  Codes: Auth(Authentication), Acct(Accounting)
         Req(Request), Accp(Accept), Rej(Reject)
         Resp(Response), COA(Change-of-Authorization)
         0(Can not exist in this packet)
         1(Can exist in this packet)
------------------------------------------------------------------------------
Attribute                  Service    Auth Auth Auth Acct Acct COA COA
Name(Type)                   Type      Req  Accp Rej  Req  Resp Req Ack
------------------------------------------------------------------------------
User-Name(1)                All       1    0    0    1    0    1    1
User-Password(2)            All       1    0    0    0    0    0    0
CHAP-Password(3)            All       1    0    0    0    0    0    0
NAS-IP-Address(4)           All       1    0    0    1    0    1    1
NAS-Port(5)                 All       1    0    0    1    0    1    1
Service-Type(6)             All       1    1    0    0    0    0    0
......
```

NOTE

The preceding information is an example. The displayed attribute type depends on the actual situation.

Table 13-23 Description of the **display radius-attribute** command output

Item	Description
0(Can not exist in this packet)	Attribute not supported in packets.
1(Can exist in this packet)	Attribute supported in packets.
Attribute Name(Type)	Attribute name and type.
Service Type	Protocol type of the attribute.
Auth Req	Authentication request packet.
Auth Accp	Authentication accept packet.

Item	Description
Auth Rej	Authentication reject packet.
Acct Req	Accounting request packet.
Acct Resp	Accounting response packet.
COA Req	Change of Authorization (COA) request packet.
COA Ack	COA acknowledgement packet.

Display the RADIUS attribute numbered 2.

```
<HUAWEI> display radius-attribute type 2
 Radius Attribute Type        : 2
 Radius Attribute Name        : User-Password
 Radius Attribute Description : This Attribute indicates the password of the user to be authenticated. Only
valid for the PAP authentication.
 Supported Packets            : Auth Request
```

Table 13-24 Description of the **display radius-attribute type** command output

Item	Description
Radius Attribute Type	Type of the RADIUS attribute.
Radius Attribute Name	Name of the RADIUS attribute.
Radius Attribute Description	Description of the RADIUS attribute.
Supported Packets	Packets that support the RADIUS attribute.

13.2.7 display radius-attribute check

Function

The **display radius-attribute check** command displays the attributes to be checked in RADIUS Access-Accept packets.

Format

display radius-attribute [**template** *template-name*] **check**

Parameters

Parameter	Description	Value
template *template-name*	Displays the RADIUS attribute check configuration of a specified RADIUS server template.	The RADIUS server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **radius-attribute check** command is executed to configure the attributes to be checked in RADIUS Access-Accept packets, you can use the **display radius-attribute check** command to view these attributes.

Example

Check the attributes to be checked in RADIUS Access-Accept packets.

```
<HUAWEI> display radius-attribute check
Server-template-name: test1
-----------------------------------------------------
check-attr
-----------------------------------------------------
Framed-Protocol
-----------------------------------------------------
```

Table 13-25 Description of the **display radius-attribute check** command output

Item	Description
Server-template-name	Name of the RADIUS server template.
check-attr	Attributes to be checked in RADIUS Access-Accept packets.
Framed-Protocol	Encapsulation protocol for services of the Frame type.

13.2.8 display radius-attribute disable

Function

The **display radius-attribute disable** command displays the disabled RADIUS attributes.

Format

display radius-attribute [**template** *template-name*] **disable**

Parameters

Parameter	Description	Value
template *template-name*	Displays the disabled RADIUS attributes in a specified RADIUS server template. If this parameter is not specified, the disabled RADIUS attributes in all the RADIUS server templates are displayed.	The value must be an existing RADIUS server template name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display radius-attribute disable** command to view the RADIUS attributes disabled by using the **radius-attribute disable** command.

To enable a RADIUS attribute, run the **undo radius-attribute disable** command in the RADIUS server template view.

Example

Display the disabled RADIUS attributes on the device.

```
<HUAWEI> display radius-attribute disable
Packet-Type: Type of the RADIUS packets to be modified. 1 indicates valid; 0 ind
icates invalid. Bit 1 to bit 4 indicate the authentication request, authenticati
on accept, accounting request, and accounting response packets.

Server-template-name: d
------------------------------------------------------------------------------
Source-Vendor-ID Source-Sub-ID Dest-Vendor-ID Dest-Sub-ID  Direct    Packet-Type
```



```
--------------------------------------------------------------------------------
0               7           0           0           send      0 0 0 0
--------------------------------------------------------------------------------
```

Table 13-26 Description of the display radius-attribute disable command output

Item	Description
Server-template-name	RADIUS server template name.
Source-Vendor-ID	Vendor ID of the source attribute.
Source-Sub-ID	ID of the source attribute's sub-attribute.
Dest-Vendor-ID	Vendor ID of the destination attribute.
Dest-Sub-ID	ID of the destination attribute's sub-attribute.
Direct	Direction in which the attribute is translated. • receive: Translates RADIUS attributes for received packets. • send: Translates RADIUS attributes for sent packets.
Packet-Type	Type of RADIUS packets. • 0: The RADIUS attributes of this type of packets are not translated. • 1: The RADIUS attributes of this type of packets are translated.

13.2.9 display radius-attribute translate

Function

The **display radius-attribute translate** command displays the RADIUS attribute translation configuration.

Format

display radius-attribute [**template** *template-name*] **translate**

Parameters

Parameter	Description	Value
template *template-name*	Displays the RADIUS attribute translation configuration of a specified RADIUS server template. *template-name* specifies the name of the RADIUS server template that is created using the **radius-server template** command. If this parameter is not specified, the disabled RADIUS attributes translation configuration in all the RADIUS server templates are displayed.	The value must be an existing RADIUS server template name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **radius-attribute translate** command to configure the device to translate RADIUS attributes, run the **display radius-attribute translate** command to check the configuration.

Example

Display the RADIUS attribute translation configuration.

```
<HUAWEI> display radius-attribute translate
Packet-Type: Type of the RADIUS packets to be modified. 1 indicates valid; 0 indicates invalid. Bit 1 to bit 4 indicate the authentication request, authentication accept, accounting request, and accounting response packets.

Server-template-name: rds
------------------------------------------------------------------------------
Source-Vendor-ID Source-Sub-ID Dest-Vendor-ID Dest-Sub-ID  Direct    Packet-Type
------------------------------------------------------------------------------
0              6            0              40           receive   0 0 0 0
------------------------------------------------------------------------------
Server-template-name: eee
------------------------------------------------------------------------------
Source-Vendor-ID Source-Sub-ID Dest-Vendor-ID Dest-Sub-ID  Direct    Packet-Type
------------------------------------------------------------------------------
234567         123          2011           20           --        0 1 0 1
------------------------------------------------------------------------------
```


Table 13-27 Description of the **display radius-attribute translate** command output

Item	Description
Server-template-name	Server template name.
Source-Vendor-ID	Vendor ID of the source attribute.
Source-Sub-ID	ID of the source attribute's sub-attribute.
Dest-Vendor-ID	Vendor ID of the destination attribute.
Dest-Sub-ID	ID of the destination attribute's sub-attribute.
Direct	Direction in which the attribute is translated. • receive: Translates RADIUS attributes for received packets. • send: Translates RADIUS attributes for sent packets.
Packet-Type	Type of RADIUS packets. • 0: The RADIUS attributes of this type of packets are not translated. • 1: The RADIUS attributes of this type of packets are translated.

13.2.10 display radius-server accounting-stop-packet

Function

The **display radius-server accounting-stop-packet** command displays information about accounting-stop packets on the RADIUS server.

Format

display radius-server accounting-stop-packet { **all** | **ip** { *ip-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Displays all the accounting-stop packets.	-
ip *ip-address*	Displays the accounting-stop packets with the specified IP address.	The value of *ip-address* is in dotted decimal notation.

Parameter	Description	Value
ip *ipv6-address*	Displays the accounting-stop packets with the specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display radius-server accounting-stop-packet** command output helps you check configurations or isolate faults.

Example

Display the accounting-stop packets with the IP address being 10.138.104.32.

```
<HUAWEI> display radius-server accounting-stop-packet ip 10.138.104.32
------------------------------------------------------------------------------
Time Stamp  Resend Times  Session Time  Username
------------------------------------------------------------------------------
1980409     6            22            g@rds
------------------------------------------------------------------------------
Total: 1, printed: 1
```

NOTE

When there are a large number of accounting-stop packets, the total number of accounting-stop packets (indicated by the **Total** field) is accurate. However, only some detailed data is displayed to ensure the user-friendly display on the CLI.

Table 13-28 Description of the display radius-server accounting-stop-packet command output

Item	Description
Time Stamp	Timestamp of an accounting-stop packet.
Resend Times	Number of times that accounting-stop packets have been retransmitted. **NOTE** In active/standby mode, the number of retransmission times on the standby control board is not updated.
Session Time	Session time, in seconds.
Username	User name.

13.2.11 display radius-server authorization configuration

Function

The **display radius-server authorization configuration** displays the configuration of a RADIUS authorization server.

Format

display radius-server authorization configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check whether the configuration of a RADIUS authorization server is correct.

Example

Display the configuration of RADIUS authorization servers.

```
<HUAWEI> display radius-server authorization configuration
--------------------------------------------------------------------------------
 Attribute decode same as template    :  N
 Attribute encode same as template    :  Y
 User information match type          :  all
 Calling-station-id decode MAC-format :  xx-xx-xx-xx-xx-xx
 Port                                 :  3799

 Bounce port disable                  :  Y
 Down port disable                    :  N
--------------------------------------------------------------------------------
 Domain name       : test.com
 IP address        : -
 Shared-key        : ****************
 Group             : -
 Protect           : Y
 VPN-instance      : -
--------------------------------------------------------------------------------
 1 RADIUS authorization server(s) in total
```


Table 13-29 Description of the **display radius-server authorization configuration** command output

Item	Description
Attribute decode same as template	Whether the device parses attributes in the RADIUS dynamic authorization packet based on the configuration in the RADIUS server template. To set this parameter, run the **radius-server authorization attribute-decode-sameastemplate** command.
Attribute encode same as template	Whether the device encapsulates attributes in the CoA or DM Response packet based on the configuration in the RADIUS server template. To set this parameter, run the **radius-server authorization attribute-encode-sameastemplate** command.
User information match type	Method in which a device checks whether the RADIUS attributes in the received CoA or DM Request packet match user information on the device: • all: The device checks whether all RADIUS attributes in the received CoA or DM Request packet match user information on the device. • any: The device checks whether a RADIUS attribute in the received CoA or DM Request packet matches user information on the device. To set this parameter, run the **radius-server authorization match-type** command.
Calling-station-id decode MAC-format	Format of the MAC address that can be parsed by the device and is configured in the system view in the Calling-Station-Id field of the CoA or DM Response packet. To set this parameter, run the **radius-server authorization calling-station-id decode-mac-format** command.
Port	Port number of a RADIUS authorization server. To set this parameter, run the **radius-server authorization port** command.

Item	Description
Bounce port disable	Whether the function of ignoring the authorization attribute indicating that the port is intermittently interrupted in a CoA packet is disabled. To set this parameter, run the **radius-server authorization hw-ext-specific command bounce-port disable** command.
Down port disable	Whether the function of ignoring the authorization attribute indicating that the port is disabled in a CoA packet is disabled. To set this parameter, run the **radius-server authorization hw-ext-specific command down-port disable** command.
Domain name	Domain name of a RADIUS accounting server.
IP-Address	IP address of a RADIUS authorization server. To set this parameter, run the **radius-server authorization** command.
Shared-key	Shared key of the RADIUS authorization server. To set this parameter, run the **radius-server authorization** command.
Group	RADIUS server group matching the RADIUS authorization server. To set this parameter, run the **radius-server authorization** command.
Protect	Whether the security hardening function is enabled. To set this parameter, run the **radius-server authorization** command.
vpn-instance	Name of the VPN instance that the RADIUS authorization server is bound to. To set this parameter, run the **radius-server authorization** command.

13.2.12 display radius-server configuration

Function

The **display radius-server configuration** command displays configuration information about a RADIUS server template.

Format

display radius-server configuration [**template** *template-name*]

Parameters

Parameter	Description	Value
template *template-name*	Specifies the name of a RADIUS server template. If this parameter is not specified, configuration information of all RADIUS server templates is displayed.	The RADIUS server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the configuration of a RADIUS server template is completed or a RADIUS fault needs to be rectified, you can run this command to check whether the configuration of the RADIUS server template is correct.

Example

Display configuration information about the RADIUS server template named **shiva**.

```
<HUAWEI> display radius-server configuration template shiva
  ------------------------------------------------------------------------------
  Server-template-name          : shiva
  Server-template-index         : 1
  Protocol-version              : standard
  Traffic-unit                  : B
  Shared-secret-key             : ******
  Group-filter                  : class
  Timeout-interval(in second)   : 5
  Retransmission                : 2
  EndPacketSendTime             : 0
```



```
Dead time(in minute)          : 5
Domain-included               : YES
NAS-IP-Address                : -
Calling-station-id MAC-format :  xxxx-xxxx-xxxx
Called-station-id MAC-format  :  XX.XX.XX.XX.XX.XX
NAS-Port-ID format            : New
Service-type                  : -
WLAN Called-station-id format :  ap-mac:ssid
NAS-IPv6-Address              : ::
Server algorithm              : master-backup
Detect-interval(in second)    : 60
Detect up-server(in second)   : 0
Detect timeout(in second)     : 3
Testuser-username             : test
Testuser-ciperpwd             : %^%#.5*EDl^j_WXg[#Z>plj8;k|8.s*ju<_F~g9k`0*9%^%#
Chargeable-user-identity      : Not Support
CUI Not reject                : No
Enable framed-ip-address      : Yes
Enable IPv4 traffic-statistics encapsulation :  No
Authentication Server 1       : 10.7.66.66     Port:1812  Weight:80  [up]
                        Vrf:- LoopBack:NULL Vlanif:NULL
                        Source IP: ::
                        Domain name: test.com
Authentication Server 2       : 10.7.66.67     Port:1812  Weight:80  [up]
                        Vrf:- LoopBack:NULL Vlanif:NULL
                        Source IP: ::
                        Domain name: test.com
Accounting Server     1       : 10.7.66.66     Port:1813  Weight:80  [up]
                        Vrf:- LoopBack:NULL Vlanif:NULL
                        Source IP: ::
Accounting Server     2       : 10.7.66.67     Port:1813  Weight:80  [up]
                        Vrf:- LoopBack:NULL Vlanif:NULL
                        Source IP: ::
------------------------------------------------------------------------------
```

Table 13-30 Description of the **display radius-server configuration template** *template-name* command output

Item	Description
Server-template-name	Name of a RADIUS server template. To set this parameter, run the **radius-server template** command.
Server-template-index	Index of a RADIUS server template.
Protocol-version	RADIUS protocol version: • standard • huawei • iphotel • portal

Item	Description
Traffic-unit	Traffic unit in the RADIUS server template. ● B: Byte ● KB: Kilobyte ● MB: Megabyte ● GB: Gigabyte To set this parameter, run the **radius-server traffic-unit** command.
Shared-secret-key	Shared key in the RADIUS server template. To set this parameter, run the **radius-server shared-key** command.
Group-filter	Filtering field of a user group. Currently, only the class field can be used as the filtering field of a user group.
Timeout-interval(in second)	Response timeout period of a RADIUS server. To set this parameter, run the **radius-server retransmit timeout** command.
Retransmission	Number of times RADIUS packets are retransmitted. To set this parameter, run the **radius-server retransmit timeout** command.
EndPacketSendTime	Number of times RADIUS accounting-stop packets are retransmitted. To set this parameter, run the **radius-server accounting-stop-packet resend** command.
Dead time(in minute)	Interval for the primary RADIUS server to revert to the active state. To set this parameter, run the **radius-server retransmit timeout** command.
Domain-included	Whether the RADIUS user name contains the domain name. ● YES: The user name contains the domain name. ● NO: The user name does not contain the domain name. ● Original: The device does not modify the user name entered by the user. To set this parameter, run the **radius-server user-name domain-included** command.

Item	Description
NAS-IP-Address	NAS IP address in RADIUS packets.
Calling-station-id MAC-format	Encapsulation format of the MAC address in the calling-station-id attribute of RADIUS packets.
Called-station-id MAC-format	Encapsulation format of the MAC address in the called-station-id attribute of RADIUS packets. To set this parameter, run the **called-station-id mac-format** command.
NAS-Port-ID format	Format of the NAS-Port-ID attribute on the RADIUS server. • New: Uses the new format of the NAS-Port-ID attribute. • New client-option82: Specifies that the content of the circuit ID suboption in the Option 82 field is encapsulated into the NAS-Port-ID attribute in a RADIUS packet. The format of the NAS-Port-ID attribute is the same as that of the suboption. • Old: Uses the old format of the NAS-Port-ID attribute. • vendor 9: Uses the NAS-Port-ID format of Cisco. To set this parameter, run the **radius-server nas-port-id-format** command.
Service-type	Service type.
WLAN Called-station-id format	Encapsulation content of the called-station-id (30) attribute in RADIUS packets. To set this parameter, run the **called-station-id wlan-user-format** command. **NOTE** Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this item.
NAS-IPv6-Address	NAS IPv6 address in RADIUS packets.

Item	Description
Server algorithm	Algorithm for selecting RADIUS servers: • master-backup: specifies the algorithm for selecting RADIUS servers as packet-based primary/secondary. • master-backup based-user: specifies the algorithm for selecting RADIUS servers as single user-based primary/secondary. • loading-share: specifies the algorithm for selecting RADIUS servers as packet-based load balancing. • loading-share based-user: specifies the algorithm for selecting RADIUS servers as single user-based load balancing. To set this parameter, run the **radius-server algorithm** command.
Detect-interval(in second)	Automatic detection interval for RADIUS servers in Down state. To set this parameter, run the **radius-server detect-server** command.
Detect up-server(in second)	Automatic detection interval for RADIUS servers in Up state. To set this parameter, run the **radius-server detect-server up-server interval** command.
Detect timeout(in second)	Timeout period for automatic RADIUS server detection packets. To set this parameter, run the **radius-server detect-server timeout** command.
Chargeable-user-identity	Whether the device supports the CUI attribute. The value can be: • Not Support: The device does not support the CUI attribute. • Support: The device supports the CUI attribute. To set this parameter, run the **radius-server support chargeable-user-identity** command.

Item	Description
CUI Not reject	Whether the device does not process the CUI attribute. The value can be: ● No: The device processes the CUI attribute. ● Yes: The device does not process the CUI attribute. To set this parameter, run the **radius-server support chargeable-user-identity** command.
Enable framed-ip-address	Whether the device is enabled to encapsulate the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address. The value can be: ● No: disabled ● Yes: enabled To set this parameter, run the **radius-server framed-ip-address no-user-ip enable** command.
Enable IPv4 traffic-statistics encapsulation	Whether the function of separately encapsulating IPv4 traffic is enabled in the RADIUS server template: ● Yes ● No
Testuser-username	User name for automatic RADIUS server detection. To set this parameter, run the **radius-server testuser** command.
Testuser-ciperpwd	User password for automatic RADIUS server detection. To set this parameter, run the **radius-server testuser** command.
Authentication Server 1	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the primary RADIUS authentication server. To set this parameter, run the **radius-server authentication** command.
Authentication Server 2	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the secondary RADIUS authentication server. To set this parameter, run the **radius-server authentication** command.

Item	Description
Accounting Server 1	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the primary RADIUS accounting server. To set this parameter, run the **radius-server accounting** command.
Accounting Server 2	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the secondary RADIUS accounting server. To set this parameter, run the **radius-server accounting** command.
Domain name	Domain name of a RADIUS accounting server.

13.2.13 display radius-server dead-interval dead-count detect-cycle

Function

The **display radius-server dead-interval dead-count detect-cycle** command displays configuration information about the RADIUS server detection interval, number of times the RADIUS server detection interval cycles, and maximum number of consecutive unacknowledged packets in each detection interval.

Format

display radius-server { **dead-interval** | **dead-count** | **detect-cycle** }

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the RADIUS server detection interval, number of times the RADIUS server detection interval cycles, and maximum number of consecutive unacknowledged packets in each detection interval are configured using the **radius-server dead-**

interval dead-count detect-cycle command, you can run the **display radius-server** { **dead-interval** | **dead-count** | **detect-cycle** } command to check configuration information about the RADIUS server detection interval, number of times the RADIUS server detection interval cycles, and maximum number of consecutive unacknowledged packets in each detection interval.

Example

Display configuration information about the RADIUS server detection interval.

```
<HUAWEI> display radius-server dead-interval
Radius server state detected internal is 5.
```

Display configuration information about the maximum number of consecutive packets that are not acknowledged by the RADIUS server in each detection interval.

```
<HUAWEI> display radius-server dead-count
Radius server state detected count is 2.
```

Display configuration information about the number of times the RADIUS server detection interval cycles.

```
<HUAWEI> display radius-server detect-cycle
Radius server down detect cycle is 2.
```

Table 13-31 Description of the **display radius-server** { **dead-interval** | **dead-count** | **detect-cycle** } command output

Item	Description
Radius server state detected internal is	Detection interval of the current RADIUS server.
Radius server state detected count is	Maximum number of consecutive packets that are not acknowledged by the RADIUS server.
Radius server down detect cycle is	Number of times the RADIUS server detection interval cycles.

13.2.14 display radius-server item

Function

The **display radius-server item** command shows the RADIUS server configuration.

Format

display radius-server item { **ip-address** { *ipv4-address* | *ipv6-address* } { **accounting** | **authentication** } | **template** *template-name* }

Parameters

Parameter	Description	Value
ip-address { *ipv4-address* | *ipv6-address* }	Specifies the IP address of the RADIUS server.	*ipv4-address*: The value is in dotted decimal notation. *ipv6-address*: The value is a 32-digit hexadecimal number.
accounting	Indicates the RADIUS accounting server.	-
authentication	Indicates the RADIUS authentication server.	-
template *template-name*	Specifies the RADIUS server template name.	The value must be an existing RADIUS server template name.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display radius-server item** command shows the RADIUS server configuration.

Example

Display the configuration of RADIUS server template **rds**.

```
<HUAWEI> display radius-server item template rds
 ------------------------------------------------------------------------------
 STState    = STState-up
 STChgTime  = -
 Type       = auth-server
 State      = state-up
 AlarmFlag  = false
 STUseNum   = 1
 IPAddress  = 192.168.30.1
 AlarmTimer = 0xffffffff
 Head       = 1057
 Tail       = 1311
 ProbeID    = 255
 Type       = acct-server
 State      = state-up
 AlarmFlag  = false
 STUseNum   = 1
 IPAddress  = 192.168.30.1
 AlarmTimer = 0xffffffff
 Head       = 1057
```



```
Tail       = 1311
ProbeID    = 255
Domain name   = test.com
------------------------------------------------------------------------------
```

Table 13-32 Description of the **display radius-server item** template command output

Item	Description
STState	RADIUS server template status: ● STState-up: indicates that the RADIUS server template is UP status. ● STState-down: indicates that the RADIUS server template is DOWN status.
STChgTime	Time when the RADIUS server template status changes.
Type	RADIUS server type: authentication or accounting server. ● auth-server: indicates authentication server. ● acct-server: indicates accounting server.
State	RADIUS server status: ● state-up: indicates the Up state. ● state-down: indicates the Down state. ● state-force-up: indicates the forcible Up state. ● state-probe: indicates the detection state.
AlarmFlag	Alarm flag. ● true: indicates that an alarm about status change has been sent. ● false: indicates that an alarm about status change is not sent.
STUseNum	RADIUS server template ID.
IPAddress	RADIUS server IP address.
AlarmTimer	ID of the alarm timer.
Head	Head pointer used to allocate the ID to RADIUS packets.
Tail	Tail pointer used to allocate the ID to RADIUS packets.
ProbeID	ID of probe packets.
Domain name	Domain name of a RADIUS accounting server.

13.2.15 display radius-server max-unresponsive-interval

Function

The **display radius-server max-unresponsive-interval** command displays configuration information about the longest unresponsive interval of a RADIUS server.

Format

display radius-server max-unresponsive-interval

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the longest unresponsive interval of a RADIUS server is configured using the **radius-server max-unresponsive-interval** command, you can run the **display radius-server max-unresponsive-interval** command to display configuration information about the longest unresponsive interval of the RADIUS server.

Example

Display configuration information about the longest unresponsive interval of the RADIUS server.

```
<HUAWEI> display radius-server max-unresponsive-interval
Radius server max non-response interval(in seconds) is 400.
```

Table 13-33 Description of the **display radius-server max-unresponsive-interval** command output

Item	Description
Radius server max non-response interval(in seconds) is	Longest unresponsive interval of the current RADIUS server.

13.2.16 display radius-server session-manage configuration

Function

The **display radius-server session-manage configuration** command displays session management configuration on the RADIUS server.

Format

display radius-server session-manage configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After session management is enabled using the **radius-server session-manage** command on the RADIUS server, you can run this command to view session management configuration.

Example

Display session management configuration on the RADIUS server.

```
<HUAWEI> display radius-server session-manage configuration
------------------------------------------------------------------------------
Session Manage Enable : True    Session Manage AnyServer : False
------------------------------------------------------------------------------
IP Address      VPN Instance                Shared-key
------------------------------------------------------------------------------
10.1.1.1        -                           ****************
------------------------------------------------------------------------------
1 Radius session manage server(s) in total
```

Table 13-34 Description of the **display radius-server session-manage configuration** command output

Item	Description
Session Manage Enable	Whether session management is enabled: • True: enabled • False: disabled To set this parameter, run the **radius-server session-manage** command.

Item	Description
Session Manage AnyServer	Whether any RADIUS session management server is configured: • True: configured • False: not configured
IP Address	IP address of the RADIUS session management server.
VPN Instance	Name of the VPN instance bound to the RADIUS session management server.
Shared-key	Shared key of the RADIUS session management server.
Radius session manage server(s) in total	Number of the RADIUS session management servers.

13.2.17 radius-attribute check

Function

The **radius-attribute check** command enables the device to check the specified attributes in the received RADIUS Access-Accept packets.

The **undo radius-attribute check** command disables the device from checking the specified attributes in the received RADIUS Access-Accept packets.

By default, the device does not check whether a RADIUS Access-Accept packet contains the specified attributes.

Format

radius-attribute check *attribute-name*

undo radius-attribute check [*attribute-name*]

Parameters

Parameter	Description	Value
attribute-name	Specifies the name of the RADIUS attribute. If this parameter is specified, the RADIUS Access-Accept packets are checked based on attribute names.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **radius-attribute check** command is executed, the device checks whether the received RADIUS Access-Accept packets contain the specified attributes. If yes, the device considers that authentication was successful; if not, the device considers that authentication failed and discards the packet. For example, after the **radius-attribute check filter-id** command is executed, the device checks the filter-id attribute in the received RADIUS Access-Accept packets. If a RADIUS packet does not contain this attribute, authentication fails.

Precautions

- When you use the **undo radius-attribute check** command with parameters, the device checks the specified attributes in the RADIUS Access-Accept packets. When you use the **undo radius-attribute check** command without any parameter, the device does not check RADIUS Access-Accept packets.
- The **display radius-attribute** can display RADIUS attribute names.

Example

Check whether the RADIUS Access-Accept packets contain the framed-protocol attribute.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-attribute check framed-protocol
```

13.2.18 radius-attribute cut hw-portal-url

Function

The **radius-attribute cut hw-portal-url** command deletes the specified content from the URL contained in the Huawei RADIUS attribute 26-156 (HW-Portal-URL).

The **undo radius-attribute cut hw-portal-url** command configures the device not to process the URL contained in the Huawei RADIUS attribute 26-156 (HW-Portal-URL).

By default, the device does not process the URL contained in the Huawei RADIUS attribute 26-156 (HW-Portal-URL).

Format

radius-attribute cut hw-portal-url *key-words* [**end** *mark*]

undo radius-attribute cut hw-portal-url

Parameters

Parameter	Description	Value
key-words	Specifies the start keyword of the content to be deleted.	The value is a string of 3 to 64 characters. It must start with an ampersand (&) and end with an equal sign (=). Spaces are not allowed.
end *mark*	Specifies the end character of the content to be deleted. If no end character is configured, all the characters following *key-words* in the URL will be deleted.	Currently, the end character can only be an ampersand (&).

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

This command is used to perform special processing on the URL delivered by the RADIUS server using the Huawei RADIUS attribute 26-156 (HW-Portal-URL) to meet interconnection requirements. Generally, this command does not need to be configured.

Example

Delete the character string **&portal=** and the content following **&portal=** from the URL contained in the Huawei RADIUS attribute 26-156 (HW-Portal-URL).

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-attribute cut hw-portal-url &portal=
```

13.2.19 radius-server max-unresponsive-interval

Function

The **radius-server max-unresponsive-interval** command displays the maximum interval during which the RADIUS server does not respond.

The **undo radius-server max-unresponsive-interval** command restores the default setting.

By default, the maximum interval during which the RADIUS server does not respond is 300 seconds.

Format

radius-server max-unresponsive-interval *interval*

undo radius-server max-unresponsive-interval

Parameters

Parameter	Description	Value
interval	Specifies the maximum interval during which the RADIUS server does not respond.	The value is an integer in the range of 10 to 7200, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the user access frequency is low and the device receives only a few authentication request packets sourced from users, the device cannot detect the RADIUS server status by periodically detecting authentication request packets. In this case, you can configure the function of setting the RADIUS server status to Down if no response is received from the server for a long period of time to ensure that users can obtain escape authorization. When the interval between two consecutive unresponded authentication request packets is greater than the interval configured using the **max-unresponsive-interval** command, the RADIUS server is set to Down.

Precautions

To check the RADIUS server status, run the **display radius-server configuration** command. If the RADIUS server status is Down, the device records logs and alarms. For details about logs, see **RDS/4/RDAUTHDOWN**. For details about alarms, see **RDS_1.3.6.1.4.1.2011.5.25.40.15.2.2.1.2 hwRadiusAuthServerDown**.

Example

Set the maximum interval during which the RADIUS server does not respond to 100s.

```
<HUAWEI> system-view
[HUAWEI] radius-server max-unresponsive-interval 100
```


13.2.20 radius-attribute disable

Function

The **radius-attribute disable** command disables a RADIUS attribute.

The **undo radius-attribute disable** command enables a disabled RADIUS attribute.

By default, no RADIUS attribute is disabled.

Format

radius-attribute disable *attribute-name* { **receive** | **send** } *

undo radius-attribute disable [*attribute-name*]

Parameters

Parameter	Description	Value
attribute-name	Specifies the name of a RADIUS attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
receive	Disables a RADIUS attribute for received packets.	-
send	Disables a RADIUS attribute for sent packets.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Generally, a RADIUS server connects to multiple network devices, which can be one vendor's devices or different vendors' devices. If some vendors' devices require the RADIUS server to deliver an attribute to support a specified feature but other vendors' device do not support the delivered attribute, the RADIUS attribute may fail to be parsed.

The device may communicate with RADIUS servers of different vendors. Some RADIUS servers require the device to send some attributes but other RADIUS servers cannot process the attributes. Errors may occur.

The **radius-attribute disable** command disables RADIUS attributes on the device. You can configure the device to ignore incompatible attributes when receiving RADIUS packets to prevent parsing failures. You can also configure the device to disable RADIUS attributes when sending RADIUS packets. When the device sends RADIUS packets, it does not encapsulate the disabled RADIUS attributes in the RADIUS packets.

Prerequisites

The RADIUS attribute translation function has been enabled using the **radius-server attribute translate** command.

Precautions

Before disabling RADIUS attributes, run the **display radius-attribute** command to view the RADIUS attributes supported by the device.

Example

Disable the Frame-Route attribute in sent packets.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server attribute translate
[HUAWEI-radius-test1] radius-attribute disable framed-route send
```

13.2.21 radius-attribute nas-ip

Function

The **radius-attribute nas-ip** command sets the NAS-IP-Address attribute in a RADIUS packet sent from an NAS.

The **undo radius-attribute nas-ip** command deletes the configured NAS-IP-Address attribute.

By default, the source IP address of the NAS is the NAS-IP-Address attribute value.

Format

radius-attribute nas-ip { *ip-address* | **ap-info** }

undo radius-attribute nas-ip [**ap-info**]

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **ap-info** parameter.

Parameters

Parameter	Description	Value
ip-address	Specifies the NAS-IP-Address attribute value in RADIUS packets sent by the device. In wireless scenarios, when a device functions as an AC, the IP address of the AC is specified as the NAS-IP-Address attribute value in RADIUS packets sent by the device.	The value is a valid unicast address in dotted decimal notation.
ap-info	The IP address of the AP is specified as the NAS-IP-Address attribute value in RADIUS packets sent by the device when the device functions as an AC in a wireless scenario.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A RADIUS server uses the NAS-IP-Address attributes in RADIUS packets sent by NASs to identify NASs. You can run the **radius-attribute nas-ip** command in the RADIUS server template view to set the NAS-IP-Address attribute.

When the RADIUS server interconnected with the device requires that the NAS-IP-Address attribute value is the IP address of the AP when the device functions as an AC in a wireless scenario, you need to run the **radius-attribute nas-ip ap-info** command.

Prerequisites

A RADIUS server template has been created using the **radius-server template** command.

Precautions

If the RADIUS NAS-IP-Address attribute is set to an invalid IP address, the configuration fails and an error message is displayed.

Example

Set the RADIUS NAS-IP-Address attribute.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-attribute nas-ip 10.3.3.3
```

13.2.22 radius-attribute nas-ipv6

Function

The **radius-attribute nas-ipv6** command sets the NAS-IPv6-Address attribute in a RADIUS packet sent from a network access server (NAS).

The **undo radius-attribute nas-ipv6** command deletes the configured NAS-IPv6-Address attribute.

By default, no NAS-IPv6-Address attribute is configured.

Format

radius-attribute nas-ipv6 *ipv6-address*

undo radius-attribute nas-ipv6

Parameters

Parameter	Description	Value
ipv6-address	Specifies the NAS-IPv6-Address attribute in a RADIUS packet.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The RADIUS server uses IP addresses to identify different NASs. The NAS-IPv6-Address attribute in a RADIUS packet can be configured using the **radius-attribute nas-ipv6** command in the RADIUS template.

Prerequisites

A RADIUS server template has been created using the **radius-server template** command.

Precautions

If the RADIUS NAS-IP-Address attribute is set to an invalid IP address, the configuration fails and an error message is displayed.

Example

Set the RADIUS NAS-IPv6-Address attribute.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-attribute nas-ipv6 FC00::7
```

13.2.23 radius-attribute service-type with-authenonly-reauthen

Function

The **radius-attribute service-type with-authenonly-reauthen** command sets the reauthentication mode to reauthentication only.

The **undo radius-attribute service-type with-authenonly-reauthen** command restores the reauthentication mode to reauthentication and reauthorization.

By default, the reauthentication mode is reauthentication and reauthorization.

Format

radius-attribute service-type with-authenonly-reauthen

undo radius-attribute service-type with-authenonly-reauthen

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user needs to be reauthenticated, the device delivers authorization information to all online users after the user is successfully authenticated. If many online users and authorization configurations exist on the device, the device

cannot promptly deliver authorization information, causing an authorization failure and user disconnection. After the **radius-attribute service-type with-authenonly-reauthen** command is run in the RADIUS server template view, the device only reauthenticates users during reauthentication, and does not redeliver authorization information, preventing users from going offline due to authorization failures.

Precautions

After the **radius-attribute service-type with-authenonly-reauthen** command is configured, users still use the original authorization information after being successfully reauthenticated even if the user authorization information changes.

This function takes effect only when the Service-Type attribute of a RADIUS server is **Authenticate Only**.

After the reauthentication mode is set to reauthentication only, the user name remains unchanged during reauthentication.

If server authorization packets carry the following attributes during reauthentication, this function does not take effect, but changes to the following authorization are still supported:

- User-Name authorized by the server
- CUI attribute authorized by the server
- Maximum number of users who are allowed to access the network using the same user name

Example

Set the reauthentication mode to reauthentication only.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] radius-attribute service-type with-authenonly-reauthen
```

13.2.24 radius-attribute set

Function

The **radius-attribute set** command modifies the RADIUS attributes.

The **undo radius-attribute set** command restores the default RADIUS attributes.

By default, values of the RADIUS attributes are not modified.

Format

radius-attribute set *attribute-name attribute-value* [**auth-type** { **dot1x** | **mac** | **portal** } | **user-type ipsession**]

undo radius-attribute set *attribute-name* [**auth-type** { **dot1x** | **mac** | **portal** } | **user-type ipsession**]

Parameters

Parameter	Description	Value
attribute-name	Specifies the name of the attribute to be modified.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name. Common attribute names are as follows: • NAS-Identifier • NAS-Port • NAS-Port-Id • NAS-Port-Type • NAS-Identifier • NAS-Port • NAS-Port-Id • NAS-Port-Type • NAS-Identifier • NAS-Port For details about other attribute names and values, see RADIUS Attributes.
attribute-value	Indicates the value of the attribute to be modified.	The value of *attribute-value* is automatically displayed.
auth-type { **dot1x** | **mac** | **portal** }	Specifies the user authentication type: • **dot1x**: 802.1X authentication • **mac**: MAC address authentication • **portal**: Portal authentication Only the Service-Type attribute supports this parameter.	-
user-type ipsession	Specifies the users with user type being IP session. Only the Service-Type attribute supports this parameter.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The RADIUS attribute values of different vendors are different. To ensure that Huawei device can successfully communicate with the devices of other vendors, run the **radius-attribute set** command to modify the RADIUS attribute values.

For example, the Huawei device uses Service-Type value 2 to indicate an authentication request from a common user by default, while a non-Huawei RADIUS server uses Service-Type value 1 to indicate an authentication request from a common user; you can run the **radius-attribute set service-type 1** command to change the Service-Type value on the device so that the device can communicate with the RADIUS server.

Precautions

- The **radius-attribute set** command can modify only the RADIUS attributes in the authentication or accounting request packets sent from a device to the RADIUS server, and cannot modify the RADIUS attributes in the packets sent from the RADIUS server to a device.

  If you run the **display radius-attribute** command to check the RADIUS attributes supported by a device and the **Auth Req** or **Acct Req** field in the command output displays 1, the RADIUS attributes supported by the device can be carried in the authentication or accounting request packets sent from the device to the RADIUS server.

  Among the RADIUS attributes that can be carried in the authentication or accounting packets sent from the device to the RADIUS server, you cannot run the **radius-attribute set** command to modify the following attributes: User-Password, Agent-Circuit-Id, Agent-Remote-Id, NAS-IP-Address, NAS-IPv6-Address, CHAP-Password, CHAP-Challenge, EAP-Message, Framed-Interface-Id, Framed-IPv6-Prefix, Message-Authenticator, State, and Class.
- The type of the attribute modified by the **radius-attribute set** command cannot be changed.
- During MAC address authentication, the default value of the RADIUS attribute Service-Type is 10. When a fixed user name is used for MAC address authentication, you need to run the **radius-attribute set service-type 2 auth-type mac** command to set the RADIUS attribute Service-Type to 2.

Example

Create the template **temp1** and set the Service-Type attribute value to 1.


```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-attribute set service-type 1
```

13.2.25 radius-attribute translate

Function

The **radius-attribute translate** command configures a RADIUS attribute to be translated.

The **undo radius-attribute translate** command cancels the configuration.

By default, no RADIUS attribute is translated.

Format

radius-attribute translate *src-attribute-name dest-attribute-name* { **receive** | **send** | **access-accept** | **access-request** | **account-request** | **account-response** } *

radius-attribute translate extend vendor-specific *src-vendor-id src-sub-id dest-attribute-name* { **access-accept** | **account-response** } *

radius-attribute translate extend *src-attribute-name* **vendor-specific** *dest-vendor-id dest-sub-id* { **access-request** | **account-request** } *

undo radius-attribute translate [*src-attribute-name*]

undo radius-attribute translate extend *src-attribute-name*

undo radius-attribute translate extend vendor-specific *src-vendor-id src-sub-id*

Parameters

Parameter	Description	Value
src-attribute-name	Specifies the name of the source attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
dest-attribute-name	Specifies the name of the destination attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
receive	Translates RADIUS attributes for received packets.	-

Parameter	Description	Value
send	Translates RADIUS attributes for sent packets.	-
access-request	Translates RADIUS attributes for Authentication Request packets.	-
account-request	Translates RADIUS attributes for Accounting Request packets.	-
access-accept	Translates RADIUS attributes for Authentication Accept packets.	-
account-response	Translates RADIUS attributes for Accounting Response packets.	-
extend	Translates extended RADIUS attributes.	-
vendor-specific *src-vendor-id src-sub-id*	Specifies the source extended attribute to be translated. ● *src-vendor-id*: The vendor ID in the extended RADIUS attributes needs to be translated. ● *src-sub-id*: The sub ID in the RADIUS attributes needs to be translated.	● The value of *src-vendor-id* is an integer ranging from 1 to 4294967295. ● The value of *src-sub-id* is an integer ranging from 1 to 255.
vendor-specific *dest-vendor-id dest-sub-id*	Specifies the destination extended attribute to be translated. ● *dest-vendor-id*: The vendor ID in the extended RADIUS attributes needs to be translated. ● *dest-sub-id*: The sub ID in the extended RADIUS attributes needs to be translated.	● The value of *dest-vendor-id* is an integer ranging from 1 to 4294967295. ● The value of *dest-sub-id* is an integer ranging from 1 to 255.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Currently, RADIUS servers of different vendors may support different RADIUS attributes and have vendor-specific RADIUS attributes. To communicate with different RADIUS servers, the device provides the RADIUS attribute translation function. After RADIUS attribute translation is enabled, the device can translate RADIUS attributes when sending or receiving packets.

RADIUS attribute translation is used in the following modes:

- Format translation for the same attribute

  This mode is widely applied. It solves the problem of compatibility because different users have different requirements for the format of a RADIUS attribute.
- Translation between different attributes

  This mode is used because different vendors have different implementations of RADIUS attributes.

  For example, the device delivers the priority of the administrator by using the Huawei proprietary attribute HW-Exec-Privilege (26-29), whereas another vendor's device delivers it by using the Login-service (15) attribute. When the device and the vendor's device use the same RADIUS server on a network, the device is required to deliver the priority of the administrator by using the Login-service (15) attribute. After the **radius-attribute translate** command is configured, the device automatically processes the Login-service attribute in the received RADIUS authentication response packet as the HW-Exec-Privilege attribute.

Prerequisites

RADIUS attribute translation has been enabled by using the **radius-server attribute translate** command.

Before configuring RADIUS attribute translation, run the **display radius-attribute** command to view the RADIUS attributes supported by the device.

Precautions

- When the device sends packets, if attribute A is to be translated to attribute B, the type of the encapsulated attribute is the same as that of attribute B but the attribute content and format are the same as those of attribute A.
- When the device receives packets, if attribute A is to be translated to attribute B, the device parses the received attribute A as attribute B.

- When the device receives packets, it cannot translate the attributes of CoA packets.
- Three commands are available to translate RADIUS attributes:
  - To translate the attributes supported by the device to other attributes also supported by the device, run the **radius-attribute translate** command.
  - To translate the non-Huawei attributes not supported by the device to the attributes supported by the device, run the **radius-attribute translate extend vendor-specific** command.
  - To translate the attributes supported by the device to the non-Huawei attributes not supported by the device, run the **radius-attribute translate extend** command.
- The RADIUS attribute consists of Type, Length, and Value fields. A device can translate a non-Huawei RADIUS attribute (specified using the *src-sub-id* and *dest-sub-id* parameters) only when the length of the Type field in the RADIUS attribute is 1 byte.
- The device can translate the RADIUS attribute only when the type of the source RADIUS attribute is the same as that of the destination RADIUS attribute. For example, the types of NAS-Identifier and NAS-Port-Id attributes are string, and they can be translated into each other. The types of NAS-Identifier and NAS-Port attributes are string and integer respectively, they cannot be translated into each other.

Example

Configure the device to translate NAS-Identifier into NAS-Port-Id when sending RADIUS packets.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-server attribute translate
[HUAWEI-radius-temp1] radius-attribute translate nas-identifier nas-port-id send
```

Translate the Cisco No. 2 attribute (vendor ID 9) in Authentication Accept and Accounting Response packets to Huawei No. 155 extended attribute HW-URL-Flag.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-server attribute translate
[HUAWEI-radius-temp1] radius-attribute translate extend Vendor-Specific 9 2 HW-URL-Flag access-accept account-response
```

Translate the Huawei No. 153 extended attribute HW-Access-Type in Authentication Request and Accounting Request packets to Cisco No. 11 attribute.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-server attribute translate
[HUAWEI-radius-temp1] radius-attribute translate extend HW-Access-Type vendor-specific 9 11 access-request account-request
```


13.2.26 radius-reject local

Function

The **radius-reject local** command configures the device to perform local authentication on administrators if administrators are rejected during RADIUS authentication.

The **undo radius-reject local** command restores the default configuration.

By default, the device does not perform local authentication on administrators if administrators are rejected during RADIUS authentication.

Format

radius-reject local

undo radius-reject local

Parameters

None

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, after the RADIUS server responds to a user with an Access-Reject packet, the authentication process ends and the user fails the authentication. If you want administrators to go online through local authentication after they are rejected during RADIUS authentication, run the **radius-reject local** command.

Precautions

- This function takes effect only for administrators.
- The authentication method must be RADIUS authentication+local authentication.

Example

Configure the device to perform local authentication on administrators if administrators are rejected during RADIUS authentication.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme authen1
[HUAWEI-aaa-authen-authen1] authentication-mode radius local
[HUAWEI-aaa-authen-authen1] radius-reject local
```


13.2.27 radius-server (aaa domain view)

Function

The **radius-server** command applies a RADIUS server template to a domain.

The **undo radius-server** command unbinds an RADIUS server template from a domain.

By default, the RADIUS server template **default** is bound to a configured domain and the domain **default**, and no RADIUS server template is bound to the domain **default_admin**.

Format

radius-server *template-name*

undo radius-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of a RADIUS server template.	The RADIUS server template must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform RADIUS authentication and accounting for users in a domain, apply a RADIUS server template to the domain. A RADIUS server template takes effect only after the RADIUS server template is applied to a domain.

Prerequisites

A RADIUS server template has been created using the **radius-server template** command.

Example

Apply the RADIUS server template **template1** to the domain **radius1**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
```



```
[HUAWEI-radius-template1] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain radius1
[HUAWEI-aaa-domain-radius1] radius-server template1
```

13.2.28 radius-server accounting

Function

The **radius-server accounting** command configures the RADIUS accounting server.

The **undo radius-server accounting** command deletes the configuration.

By default, no RADIUS accounting server is configured.

Format

radius-server accounting *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server accounting *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server accounting *domain-name port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

undo radius-server accounting [*ipv4-address* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

undo radius-server accounting [*ipv6-address* [*port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight**]]]

undo radius-server accounting [*domain-name* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS accounting server.	The value is in dotted decimal notation. It must be a valid unicast address.
ipv6-address	Specifies the IPv6 address of a RADIUS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
domain-name	Specifies the domain name of a RADIUS accounting server.	The value is a string of 1 to 255 case-sensitive characters. It cannot contain spaces. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).
port	Specifies the port number of a RADIUS accounting server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS accounting server is bound to.	The value must be an existing VPN instance name.
source loopback *interface-number*	Specifies the number of a loopback interface.	The loopback interface must exist.
source ip-address *ipv4-address*	Specifies the source IPv4 address in RADIUS packets sent from the device to a RADIUS accounting server. If this parameter is specified, ensure that the value of this parameter is the same as the client's IPv4 address specified on the RADIUS accounting server. If this parameter is not specified, the IPv4 address of the outbound interface is used as the source IPv4 address in RADIUS packets sent from the device to a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.

Parameter	Description	Value
source ip-address *ipv6-address*	Specifies the source IPv6 address in RADIUS packets sent from the device to a RADIUS accounting server. If this parameter is not specified, the IPv6 address of the outbound interface is used as the source IPv6 address in RADIUS packets sent from the device to a RADIUS accounting server. This address cannot be a virtual IPv6 address of a VRRP6 group.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
source vlanif *interface-number*	Specifies the IP address of a VLANIF interface as the source IP address. *interface-number* specifies the number of a VLANIF interface.	The VLANIF interface must exist.
weight *weight-value*	Specifies the weight of a RADIUS accounting server. When multiple servers are available, the device uses the server with the highest weight to perform accounting. If the servers have the same weights, the device uses the server configured first to perform accounting. If this parameter is not specified, the default weight of an accounting server is 80.	The value is an integer that ranges from 0 to 100. The default value is 80.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform accounting for users, configure a RADIUS accounting server. The device communicates with a RADIUS accounting server to obtain accounting information, and performs accounting for users based on the accounting information. The device sends accounting packets to the RADIUS accounting server only after the IP address and port number of the RADIUS accounting server are specified in the RADIUS server template.

Precautions

- The IP address of the primary accounting server must be different from the IP address of the secondary accounting server; otherwise, the configuration fails.
- When the **radius-server algorithm master-backup** command has been executed to set the algorithm for selecting RADIUS servers to primary/secondary and both the primary and secondary accounting servers have been configured, the device sends accounting request packets to the secondary accounting server when the following two conditions are met:
  a. The primary server does not send any accounting response packet.
  b. The maximum number of times that the device retransmits authentication and accounting packets is reached.
- For the RADIUS server in Down status, if configuration parameters except **weight** of the RADIUS server are modified, the server status will change from Down to Up.
- The modification of the weight parameter takes effect only for the users who go online after the modification. The users who go online before the modification still send authentication and accounting packets to the selected RADIUS server.
- If the source IP address configured using this command does not exist locally, this IP address does not take effect.

  NOTE

  This restriction applies only to the following models:

  S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S
- When configuring the IP address of a RADIUS accounting server, you can configure both an IPv4 and an IPv6 address but do not configure both a domain name and IP address.
- Only IPv4 addresses can be resolved for domain names.

Example

Configure the primary RADIUS accounting server.


```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server accounting 10.163.155.12 1813
```

Configure the secondary RADIUS accounting server.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server accounting 10.163.155.15 1813 weight 50
```

Configure the domain name of a RADIUS accounting server.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server accounting www.example.com 1813
```

13.2.29 radius-server accounting-stop-packet resend

Function

The **radius-server accounting-stop-packet resend** command enables retransmission of accounting-stop packets and sets the number of accounting-stop packets that can be retransmitted each time.

The **undo radius-server accounting-stop-packet resend** command disables retransmission of accounting-stop packets.

By default, retransmission of accounting-stop packets is enabled, and the retransmission times is 3.

NOTE

The default settings are recommended. If accounting-stop packets need to be retransmitted many times, the RADIUS authentication performance of the switch will be affected and even cause a failure to send accounting-stop packets.

Format

radius-server accounting-stop-packet resend [*resend-times*]

undo radius-server accounting-stop-packet resend

Parameters

Parameter	Description	Value
resend-times	Specifies the number of accounting-stop packets that can be retransmitted each time.	The value is an integer that ranges from 0 to 300.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

When accounting-stop packets cannot be sent to the RADIUS server that is unreachable, you can run the **radius-server accounting-stop-packet resend** command to save the accounting-stop packets in the buffer and send them at the preset intervals until the number of allowed retransmission times is reached or the packets are sent successfully.

Example

Enable the retransmission of accounting-stop packets and set the number of accounting-stop packets that can be retransmitted each time to 50.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server accounting-stop-packet resend 50
```

13.2.30 radius-server algorithm

Function

The **radius-server algorithm** command configures the algorithm for selecting RADIUS servers.

The **undo radius-server algorithm** command restores the default algorithm for selecting RADIUS servers.

By default, the algorithm for selecting RADIUS servers is the single user-based primary/secondary algorithm.

Format

radius-server algorithm { **loading-share** | **master-backup** } [**based-user**]

undo radius-server algorithm

Parameters

Parameter	Description	Value
loading-share	Sets the algorithm for selecting RADIUS servers to load balancing.	-
master-backup	Sets the algorithm for selecting RADIUS servers to primary/secondary.	-

Parameter	Description	Value
based-user	Sets the algorithm for selecting RADIUS servers to the single user-based algorithm. If this parameter is not specified, the algorithm for selecting RADIUS servers is the packet-based algorithm.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When two or more than two RADIUS servers are available, you can use the **radius-server algorithm** command to set the algorithm for selecting RADIUS servers.

- When **master-backup** is specified, the weight is used to determine the primary and secondary RADIUS authentication or accounting servers. The server with a larger weight value is the primary server. If devices have the same weight, the server that was first configured is the primary server.
- When **loading-share** is specified, the device sends a packet to a server according to the weights configured on servers. For example, if the weights of RADIUS server A, RADIUS server B, and RADIUS server C are 80, 80, and 40 respectively, the probabilities of sending packets to RADIUS server A, RADIUS server B, and RADIUS server C are as follows:
  - RADIUS server A: 80/(80 + 80 + 40) = 40%
  - RADIUS server B: 80/(80 + 80 + 40) = 40%
  - RADIUS server C: 40/(80 + 80 + 40) = 20%

Authentication server information is saved in the authentication phase. If the authentication server is also the accounting server, accounting requests are first sent to this server in the accounting phase. If the accounting packets of the authentication server are unreachable, the accounting server is reselected in the accounting phase. In this case, authentication and accounting of the same user may be performed on different servers.

Precautions

If you run the **radius-server algorithm** command multiple times in the same RADIUS server template view, only the latest configuration takes effect.

Example

Set the algorithm for selecting RADIUS servers to load balancing.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server algorithm loading-share
```

13.2.31 radius-server attribute message-authenticator access-request

Function

The **radius-server attribute message-authenticator access-request** command carries the Message-Authenticator attribute in RADIUS authentication packets sent by the device.

The **undo radius-server attribute message-authenticator access-request** command cancels the Message-Authenticator attribute from RADIUS authentication packets sent by the device.

By default, RADIUS authentication packets do not carry the Message-Authenticator attribute.

Format

radius-server attribute message-authenticator access-request

undo radius-server attribute message-authenticator access-request

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The Message-Authenticator attribute is used to identify and verify authentication packets to prevent invalid packets.

NOTE

- This command is used when the PAP or CHAP authentication is enabled.
- When EAP authentication is enabled, RADIUS packets contain the Message-Authenticator attribute by default. You do not need to run this command.

Example

Configure the Message-Authenticator attribute to RADIUS authentication packets.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server attribute message-authenticator access-request
```

13.2.32 radius-server attribute translate

Function

The **radius-server attribute translate** command enables RADIUS attribute translation.

The **undo radius-server attribute translate** command disables RADIUS attribute translation.

By default, RADIUS attribute translation is disabled.

Format

radius-server attribute translate

undo radius-server attribute translate

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Currently, RADIUS servers of different vendors may support different RADIUS attributes and have vendor-specific RADIUS attributes. To communicate with different RADIUS servers, the device provides the RADIUS attribute translation function. After RADIUS attribute translation is enabled, the device can translate RADIUS attributes when sending or receiving packets.

Follow-up Procedure

After RADIUS attribute translation is enabled, perform either of the following operations to make the function to take effect:

- Run the **radius-attribute translate** command to specify the RADIUS attributes that you want to translate.

- Run the **radius-attribute disable** command to specify the RADIUS attributes that you do not want to translate.

Example

Enable RADIUS attribute translation.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server attribute translate
```

13.2.33 radius-server authentication

Function

The **radius-server authentication** command configures a RADIUS authentication server.

The **undo radius-server authentication** command deletes the configured RADIUS authentication server.

By default, no RADIUS authentication server is specified.

Format

radius-server authentication *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server authentication *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server authentication *domain-name port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

undo radius-server authentication [*ipv4-address* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

undo radius-server authentication [*ipv6-address* [*port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight**]]]

undo radius-server authentication [*domain-name* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a RADIUS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
domain-name	Specifies the domain name of a RADIUS authentication server.	The value is a string of 1 to 255 case-sensitive characters. It cannot contain spaces. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).
port	Specifies the port number of a RADIUS authentication server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authentication server is bound to.	The value must be an existing VPN instance name.
source loopback *interface-number*	Specifies the IP address of the loopback interface taken as the source IP address. *interface-number* specifies the number of a loopback interface.	The loopback interface must already exist.

Parameter	Description	Value
source ip-address *ipv4-address*	Specifies the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is specified, ensure that the value of this parameter is the same as the client's IPv4 address specified on the RADIUS authentication server. If this parameter is not specified, the IPv4 address of the outbound interface is used as the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.
source ip-address *ipv6-address*	Specifies the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is not specified, the IPv6 address of the outbound interface is used as the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server. This address cannot be a virtual IPv6 address of a VRRP6 group.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
source vlanif *interface-number*	Specifies the IP address of a VLANIF interface as the source IP address. *interface-number* specifies the number of a VLANIF interface.	The VLANIF interface must exist.

Parameter	Description	Value
weight *weight-value*	Specifies the weight of a RADIUS authentication server. When multiple servers are available, the device uses the server with the highest weight to perform authentication. If the servers have the same weights, the device uses the server configured first to perform authentication.	The value is an integer that ranges from 0 to 100. The default value is 80.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform RADIUS authentication, configure a RADIUS authentication server in a RADIUS server template. The device uses the RADIUS protocol to communicate with a RADIUS authentication server to obtain authentication information, and authenticates users based on the authentication information. The device sends authentication packets to the RADIUS authentication server only after the IP address and port number of the RADIUS authentication server are specified in the RADIUS server template.

When the **radius-server algorithm master-backup** command has been executed to set the algorithm for selecting RADIUS servers to primary/secondary and both the primary and secondary authentication servers have been configured, the device sends authentication request packets to the secondary authentication server when the following two conditions are met:

1. The primary authentication server does not send any authentication response packet.
2. The maximum number of times that the device retransmits authentication request packets is reached.

When the 802.1X authentication mode is set to EAP, the device and RADIUS authentication servers exchange packets multiple times. During the first exchange process, the device sends a request packet to the primary RADIUS authentication server. If the device resends the request packet for the maximum number of times but does not receive a response packet from the primary RADIUS authentication

server, the device sends a request packet to the secondary RADIUS authentication server. If the secondary RADIUS authentication server sends a response packet to the device, the device will directly send request packets to the secondary RADIUS authentication server in the following exchange processes. In this way, the device does not need to send a request packet to the primary RADIUS authentication server first in the following exchange processes, shortening the authentication time and preventing the user authentication connection from being disconnected because the client does not receive a response packet for a long time.

Precautions

- For the RADIUS server in Down status, if configuration parameters except **weight** of the RADIUS server are modified, the server status will change from Down to Up.
- If an interface connecting the device to a server has multiple IP addresses configured and can communicate with the server only through some of these IP addresses, one IP address among these reachable IP addresses needs to be specified as the source IP address based on the routing table to ensure that the device can communicate with the server.
- The modification of the weight parameter takes effect only for the users who go online after the modification. The users who go online before the modification still send authentication and accounting packets to the selected RADIUS server.
- You are advised to configure different RADIUS servers for the source VLANIF interface, source IP address, and source loopback interface and bind the servers to the same RADIUS template. Otherwise, the device creates multiple RADIUS servers even if the source and destination IP addresses of RADIUS request packets sent by different RADIUS templates are the same. As a result, only the first created RADIUS server receives RADIUS response packets, while other RADIUS servers cannot. To check the RADIUS server configuration, run the **display radius-server item ip-address** { *ipv4-address* | *ipv6-address* } **authentication** command.
- The management interface MEth0/0/1 cannot be used as the source interface for RADIUS authentication.
- If the source IP address configured using this command does not exist locally, this IP address does not take effect.

  NOTE

  This restriction applies only to the following models:

  S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S
- When configuring the IP address of a RADIUS authentication server, you can configure both an IPv4 and an IPv6 address but do not configure both a domain name and IP address.
- Only IPv4 addresses can be resolved for domain names.

Example

Configure the IP address of the primary RADIUS authentication server to 10.163.155.13 and the port number to 1812.


```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server authentication 10.163.155.13 1812
```

Configure the IP address of the secondary RADIUS authentication server to 10.163.155.15, the port number to 1812 and the weigh to 50.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server authentication 10.163.155.15 1812 weight 50
```

Set the domain name and port number of a RADIUS authentication server to **www.example.com** and 1812.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server authentication www.example.com 1812
```

13.2.34 radius-server authorization

Function

The **radius-server authorization** command configures the RADIUS authorization server.

The **undo radius-server authorization** command deletes the configured RADIUS authorization server.

By default, no RADIUS authorization server is configured.

Format

radius-server authorization *ip-address* [**vpn-instance** *vpn-instance-name*] { **server-group** *group-name* **shared-key cipher** *key-string* | **shared-key cipher** *key-string* [**server-group** *group-name*] } [**protect enable**]

radius-server authorization *domain-name* [**vpn-instance** *vpn-instance-name*] { **server-group** *group-name* **shared-key cipher** *key-string* | **shared-key cipher** *key-string* [**server-group** *group-name*] } [**protect enable**]

undo radius-server authorization { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] }

undo radius-server authorization { **all** | *domain-name* [**vpn-instance** *vpn-instance-name*] }

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a RADIUS authorization server.	The value is a unicast address in dotted decimal notation.

Parameter	Description	Value
domain-name	Specifies the domain name of a RADIUS authorization server.	The value is a string of 1 to 255 case-sensitive characters. It cannot contain spaces. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authorization server is bound to.	The value must be an existing VPN instance name.
server-group *group-name*	Specifies the name of a RADIUS group corresponding to a RADIUS server template.	The value is a string of 1 to 32 characters, including letters (case-sensitive), numerals (0 to 9), periods (.), hyphens (-), and underscores (_). The value cannot be - or --.
shared-key cipher *key-string*	Specifies the shared key of a RADIUS server.	The value is a case-sensitive character string without spaces or question marks (?). *key-string* can be a string of 1 to 128 characters in plaintext or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in ciphertext.
protect enable	Enables the security hardening function.	-
all	Deletes all RADIUS authorization servers.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An independent RADIUS authorization server can be used to authorize online users. RADIUS provides two authorization methods: Change of Authorization (CoA) and Disconnect Message (DM).

- CoA: After a user is successfully authenticated, you can modify the rights of the online user through the RADIUS authorization server. For example, a VLAN ID can be delivered to access users of a certain department through CoA packets, so that they belong to the same VLAN no matter which interfaces they connect to.
- DM: The administrator can forcibly disconnect a user through the RADIUS authorization server.

After the parameters such as IP address and shared key are configured for the RADIUS authorization server, the device can receive authorization requests from the server and grant rights to users according to the authorization information. After authorization is complete, the device returns authorization response packets carrying the results to the server.

After the security hardening function is enabled by specifying the **protect enable** parameter, the following occurs:

- When a CoA or DM request packet carries the Message-Authenticator attribute, the device checks the Message-Authenticator attribute. If the check fails, the device discards the request packet and does not respond the packet. If the check succeeds, the device sends a CoA or DM response packet (ACK or NAK) that carries the Message-Authenticator attribute.
- When a CoA or DM request packet does not carry the Message-Authenticator attribute, the device does not check the attribute and sends a CoA or DM response packet (ACK or NAK) that does not carry the Message-Authenticator attribute.

NOTE

When a CoA or DM request packet carries the Message-Authenticator attribute, if the **radius-attribute disable message-authenticator receive** command is configured, the device does not check the attribute and sends a response packet that does not carry the Message-Authenticator attribute; if the **radius-attribute disable message-authenticator send** command is configured, the device sends a response packet that does not carry the Message-Authenticator attribute even if the attribute check succeeds.

Precautions

To improve security, it is recommended that the password contains at least three types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 16 characters.

You also need to run the **radius-server authorization server-source** command in V200R020C10SPC100 and later versions to configure an IPv4 address for receiving and responding to request packets of a RADIUS authorization server so that the function of the RADIUS authorization server can take effect.

During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

When configuring the IP address of a RADIUS authorization server, do not configure both a domain name and IP address. Otherwise, the system prompts that the configuration fails.

Example

Specify a RADIUS authorization server.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization 10.1.1.116 shared-key cipher YsHsjx_202206
```

Configure the domain name of a RADIUS authorization server.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization www.example.com shared-key cipher YsHsjx_202206
```

13.2.35 radius-server authorization attribute-decode-sameastemplate

Function

The **radius-server authorization attribute-decode-sameastemplate** command configures the device to parse RADIUS dynamic authorization packet attributes based on the configuration in RADIUS server template.

The **undo radius-server authorization attribute-decode-sameastemplate** command restores the default method of parsing RADIUS authorization packet attributes.

By default, the device parses the MAC address in the calling-station-id attribute carried in RADIUS dynamic authorization packets based on the MAC address length, without considering the MAC address format and delimiter.

Format

radius-server authorization attribute-decode-sameastemplate

undo radius-server authorization attribute-decode-sameastemplate

Parameters

None.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device parses the MAC address in the Calling-Station-Id attribute in RADIUS dynamic authorization packets. By default, the MAC address format that can be parsed is configured using the **radius-server authorization calling-station-id decode-mac-format** command in the system view. When the device is connected to multiple RADIUS servers, the MAC address formats are different in the Calling-Station-Id attribute in dynamic authorization packets sent by different RADIUS servers. In this case, the MAC address may fail to be parsed if the same parse mode is used, resulting in that the device fails to be connected to some RADIUS servers. You can run the **radius-server authorization attribute-decode-sameastemplate** command to configure the device to parse RADIUS dynamic authorization packet attributes based on the Calling-Station-Id attribute encapsulation mode configured in each RADIUS server template, making the device be successfully connected to multiple RADIUS servers.

Prerequisites

This function is used to make the Calling-Station-Id attribute parse mode the same as the Calling-Station-Id attribute encapsulation mode configured in RADIUS server template. Therefore, make sure that the following steps have been performed before using this function.

1. The **calling-station-id mac-format** command has been run in the RADIUS server template view to configure the encapsulation mode of the MAC address in the Calling-Station-Id attribute.
2. The **radius-server authorization** command has been run in the system view to configure the authorization server to use the RADIUS server template **server-group**.

NOTE

If the RADIUS server template used by the authorization server is not specified, this function cannot be implemented on a device. You can run the **radius-server authorization calling-station-id decode-mac-format** command in the system view to configure the Calling-Station-Id attribute parse mode.

Precautions

The configuration in a RADIUS server template has a higher priority than the global configuration.

Example

Configure the RADIUS authorization server to parse attributes depending on the configuration in a RADIUS template.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization attribute-decode-sameastemplate
```

13.2.36 radius-server authorization attribute-encode-sameastemplate

Function

The **radius-server authorization attribute-encode-sameastemplate** command configures a device to encapsulate attributes in the COA or DM Response packet based on the configurations in the RADIUS server template.

The **undo radius-server authorization attribute-encode-sameastemplate** command restores the default setting.

By default, a device is not configured to encapsulate attributes in the COA or DM Response packet based on the configurations in the RADIUS server template.

Format

radius-server authorization attribute-encode-sameastemplate

undo radius-server authorization attribute-encode-sameastemplate

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The attribute match check function is configured on the RADIUS servers of some vendors. The attribute match check succeeds and the RADIUS server successfully interconnects with a device to implement dynamic authorization or offline operations only when the attribute encapsulation formats in the COA or DM Response packet received by the RADIUS server are the same as those parsed from the RADIUS authentication Response packets. The RADIUS server encapsulates the attributes parsed from the RADIUS Response packet based on the configurations in the RADIUS server template. To ensure that the attribute formats in the COA or DM Response packet are the same as those parsed by the RADIUS server from the RADIUS packet, you can run the **radius-server authorization attribute-encode-sameastemplate** command to configure the device to encapsulate attributes in the COA or DM Response packet based on the configurations in the RADIUS server template, so that the device is successfully interconnected with the RADIUS server.

Attributes whose encapsulation formats need to be configured in the COA or DM Response packet include Calling-Station-Id (31), NAS-IP-Address (4), and User-Name (1).

Precautions

- This function is used to configure the encapsulation modes of the Calling-Station-Id (31), NAS-IP-Address (4), and User-Name (1) attributes in the COA or DM Response packet to be the same as those configured in the RADIUS server template. Therefore, perform the following steps before using this function.
  a. Configure the encapsulation modes of attributes in the RADIUS server template view.

- Run the **calling-station-id mac-format** command to configure the encapsulation mode of the MAC address in the Calling-Station-Id attribute.
- Run the **radius-attribute nas-ip** command to configure the NAS-IP-Address attribute in a RADIUS packet sent from an NAS.
- Run the **radius-server user-name domain-included** command to configure whether the user name carried in the RADIUS packet contains a domain name.

b. Run the **radius-server authorization** command in the system view to configure the authorization server to use the RADIUS server template **server-group**.

- After this function is configured, the priority of the NAS IP address in the NAS-IP-Address (4) attribute is as follows: NAS IP address configured in the RADIUS server template>source IP address configured on the accounting server>source IP address configured on the authentication server>destination IP address of the Request packet
- If the **radius-server authorization attribute-encode-sameastemplate** command is not configured, no RADIUS server template is bound to the authorization server, or no attribute format configuration exists in the RADIUS server template, the formats of COA or DM response packets are as follows:
  - MAC address in the Calling-Station-Id (31) attribute: The MAC address is encapsulated in the default format XXXXXXXXXXXX.
  - NAS IP address in the NAS-IP-Address (4) attribute: destination IP address in the Request packet
  - User name in the User-Name (1) attribute: The user name in the Request packet is used.

Example

Configure the RADIUS authorization server to parse attributes based on the configurations in the RADIUS server template.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization attribute-encode-sameastemplate
```

13.2.37 radius-server authorization calling-station-id decode-mac-format

Function

The **radius-server authorization calling-station-id decode-mac-format** command sets the format of MAC address that can be parsed by a device in the calling-station-id (Type 31) attribute carried in RADIUS authorization packets.

The **undo radius-server authorization calling-station-id decode-mac-format** command restores the default format of the MAC address in the calling-station-id (Type 31) attribute.

By default, the device parses the MAC address in the calling-station-id attribute carried in RADIUS dynamic authorization packets into ASCII format, and the MAC

address does not contain separators. In addition, the device parses the MAC address in the calling-station-id attribute carried in RADIUS dynamic authorization packets based on the MAC address length, without considering the MAC address format and delimiter.

Format

radius-server authorization calling-station-id decode-mac-format { **bin** | **ascii** { **unformatted** | { **dot-split** | **hyphen-split** } [**common** | **compress**] } }

undo radius-server authorization calling-station-id decode-mac-format

Parameters

Parameter	Description	Value
bin	Indicates that the MAC address in the calling-station-id attribute uses the binary format.	-
ascii	Indicates that the MAC address in the calling-station-id attribute uses the ASCII format.	-
unformatted	Indicates that no separator is used in the MAC address in the calling-station-id field.	-
dot-split	Indicates that dots are used as the separators in MAC address.	-
hyphen-split	Indicates that the hyphens are used as the separators in MAC address.	-
common	Indicates that the MAC address in the calling-station-id attribute uses the xx-xx-xx-xx-xx-xx or xx.xx.xx.xx.xx.xx format.	-
compress	Indicates that the MAC address in the calling-station-id attribute uses the xxxx-xxxx-xxxx or xxxx.xxxx.xxxx format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the MAC address format in the calling-station-id attribute carried in RADIUS dynamic authorization packets is xxxxxxxxxxxx. If the MAC address format in the calling-station-id attribute sent by the RADIUS server is not the default format used on the device, run the **radius-server authorization calling-station-id decode-mac-format** command to change the MAC address format on the device.

When a device connects to multiple RADIUS servers, the RADIUS servers may send MAC addresses in different formats in the calling-station-id attribute to the device. You need to run the **radius-server authorization attribute-decode-sameastemplate** command to configure the device to parse the RADIUS authorization packet attributes based on the configuration in RADIUS server template, so that the device can work with these RADIUS servers.

Precautions

The configuration in a RADIUS server template has a higher priority than the global configuration.

Example

Set the format of MAC address that can be parsed by the device in the calling-station-id attribute to binary.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization calling-station-id decode-mac-format bin
```

13.2.38 radius-server authorization hw-ext-specific command bounce-port disable

Function

The **radius-server authorization hw-ext-specific command bounce-port disable** command configures the function of ignoring the authorization attribute indicating that the port goes Down intermittently in a CoA packet.

The **undo radius-server authorization hw-ext-specific command bounce-port disable** command restores the default setting.

By default, the device supports the authorization attribute indicating that the port goes Down intermittently in a CoA packet.

Format

radius-server authorization hw-ext-specific command bounce-port disable

undo radius-server authorization hw-ext-specific command bounce-port disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The value of the user-command field in the RADIUS attribute **HW-Ext-Specific(26-238)** carried in a CoA packet can be:

- 1: Indicates that user reauthentication will be performed.
- 2: Indicates that the port where the authorized user resides goes Down intermittently.
- 3: Indicates that the port where the authorized user resides is disabled.

After the server authorizes a VLAN, the VLAN to which the terminal belongs will be changed. However, the terminal does not proactively trigger an IP address reapplication event using DHCP and you must manually trigger such an event on the terminal. Such operations cannot be directly performed on dumb terminals such as printers. You can disconnect the authentication port intermittently to trigger terminals connected to the authentication port to re-apply for an IP address. To configure the function of intermittently disconnecting the authentication port, you need to run the **undo radius-server authorization hw-ext-specific command bounce-port disable** command on the device, and set the value of the RADIUS attribute HW-Ext-Specific (26-238) on the server to user-command=2.

Precautions

Pay attention to the following points if the value of the user-command field in the RADIUS attribute **HW-Ext-Specific(26-238)** carried in a CoA packet sent by the RADIUS server is 2 or 3:

- Ensure that only one user resides on the authentication port or the user to be authenticated is directly connected to the authentication port; otherwise, other users on the authentication port will be affected if the port goes Down intermittently or disabled.
- Only a physical port can function as the authentication port, while an Eth-Trunk interface cannot.
- When the value is 2, SVF and policy association are both supported. When the value is 3, SVF and policy association are not supported.

Example

Configure the function of ignoring the authorization attribute indicating that the port goes Down intermittently in a CoA packet.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization hw-ext-specific command bounce-port disable
```


13.2.39 radius-server authorization hw-ext-specific command down-port disable

Function

The **radius-server authorization hw-ext-specific command down-port disable** command configures the function of ignoring the authorization attribute indicating that the port is disabled in a CoA packet.

The **undo radius-server authorization hw-ext-specific command down-port disable** command restores the default setting.

By default, the device supports the authorization attribute indicating that the port is disabled in a CoA packet.

Format

radius-server authorization hw-ext-specific command down-port disable

undo radius-server authorization hw-ext-specific command down-port disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The value of the user-command field in the RADIUS attribute **HW-Ext-Specific(26-238)** carried in a CoA packet can be:

- 1: Indicates that user reauthentication will be performed.
- 2: Indicates that the port where the authorized user resides goes Down intermittently.
- 3: Indicates that the port where the authorized user resides is disabled.

When the value of the user-command field in a CoA packet sent by the RADIUS server is 3, users go offline and their network access rights are blocked. The most obvious impact of this is that the port where the authorized user resides is disabled. If you want to enable this port, you have to log in to the device to manually enable it. To avoid unintentionally making users go offline, you can disable the authorization attribute in a CoA packet indicating that the port is disabled by running the **radius-server authorization hw-ext-specific command down-port disable** command.

Precautions

Pay attention to the following points if the value of the user-command field in the RADIUS attribute **HW-Ext-Specific(26-238)** carried in a CoA packet sent by the RADIUS server is 2 or 3:

- Ensure that only one user resides on the authentication port or the user to be authenticated is directly connected to the authentication port; otherwise, other users on the authentication port will be affected if the port goes Down intermittently or disabled.
- Only a physical port can function as the authentication port, while an Eth-Trunk interface cannot.
- When the value is 2, SVF and policy association are both supported. When the value is 3, SVF and policy association are not supported.

Example

Configure the function of ignoring the authorization attribute indicating that the port is disabled in a CoA packet.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization hw-ext-specific command down-port disable
```

13.2.40 radius-server authorization match-type

Function

The **radius-server authorization match-type** command configures the method in which the device checks whether the RADIUS attributes in the received CoA or DM Request packet match user information on the device.

The **undo radius-server authorization match-type** command restores the default setting.

By default, a device checks whether the RADIUS attributes in the received CoA or DM Request packet match user information on the device using the **any** method, namely, the device checks whether a specific RADIUS attribute in the received CoA or DM Request packet matches user information on the device.

Format

radius-server authorization match-type { **any** | **all** }

undo radius-server authorization match-type

Parameters

Parameter	Description	Value
any	Indicates that the device checks whether a specified attribute matches user information on the device.	-

Parameter	Description	Value
all	Indicates that the device checks whether all attributes match user information on the device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A device checks whether the RADIUS attributes in the CoA or DM Request packet match user information on the device to identify users in the following two methods:

- **any** method: The device checks whether an attribute matches user information on the device. The priority of identifying the RADIUS attributes used by the users is as follows: Acct-Session-ID (44) > Calling-Station-Id (31) > Framed-IP-Address (8). The device searches for the attributes in the Request packet based on the priority, and matches the first found attribute against user information on the device. If the attribute is successfully matched, the device responds with an ACK packet; otherwise, the device responds with a NAK packet.
- **all** method: The device checks whether all attributes match user information on the device. It identifies the following RADIUS attributes used by users in the listed order: Acct-Session-ID (44), Calling-Station-Id (31), Framed-IP-Address (8), and User-Name (1). The device matches one or more of the preceding attributes in the Request packet against user information on the device. If all the attributes are successfully matched, the device responds with an ACK packet; otherwise, the device responds with a NAK packet.

Precautions

When the RADIUS attribute translation function is configured in the RADIUS template using the **radius-attribute translate** command, the match will fail.

Currently, the **any** method supports only the Acct-Session-ID (44), Calling-Station-Id (31), and Framed-IP-Address (8) attributes. The device does not match other attributes against user information on the device.

Example

Configure the device to check whether all RADIUS attributes in the received CoA or DM Request packet match user information on the device.


```
<HUAWEI> system-view
[HUAWEI] radius-server authorization match-type all
```

13.2.41 radius-server authorization port

Function

The **radius-server authorization port** command configures the port ID of the RADIUS authorization server.

The **undo radius-server authorization Port** command restores the default setting.

By default, the port ID of the RADIUS authorization server is 3799.

Format

radius-server authorization port *port-id*

undo radius-server authorization port

Parameters

Parameter	Description	Value
port-id	Specifies the port ID of the RADIUS authorization server.	The value is an integer that ranges from 1024 to 55535, and the default value is 3799.

Views

System view

Default Level

3: Management level

Usage Guidelines

Run the **radius-server authorization port** *port-id* command to configure the port ID that a device uses when sending packets to the RADIUS authorization server. The device then uses the configured port ID as the destination port ID to send Response packets to the RADIUS authorization server after receiving COA or DM Request packets from the RADIUS authorization server.

Example

Set the port ID of the RADIUS authorization server to 3700.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization port 3700
```


13.2.42 radius-server authorization server-source

Function

The **radius-server authorization server-source** command configures an IPv4 address for receiving and responding to request packets of a RADIUS authorization server.

The **undo radius-server authorization server-source** command restores the default setting.

By default, the device does not receive or respond to any request packet of a RADIUS authorization server.

Format

radius-server authorization server-source { **ip-address** *ip-address* | **all-interface** }

undo radius-server authorization server-source { **ip-address** *ip-address* | **all-interface** | **all** }

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation.
all-interface	Specifies the IPv4 address as 0.0.0.0. That is, the device receives and responds to request packets of a RADIUS authorization server through any IPv4 address.	-
all	Indicates all IPv4 addresses specified by **ip-address** *ip-address*.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no IPv4 address can be used to receive or respond to request packets of the RADIUS authorization server. When the device needs to establish a connection with a RADIUS authorization server, you can run the **radius-server authorization server-source** command to specify an IPv4 address for the device to receive and respond to request packets of the RADIUS authorization server.

Precautions

- After you run this command to configure an IPv4 address for the device to receive and respond to request packets of a RADIUS authorization server, the RADIUS authorization server can communicate with the device only through this IPv4 address. Ensure that the RADIUS authorization server can communicate with the device through this IPv4 address at Layer 3.
- After the **radius-server authorization server-source all-interface** command is run, the device receives and responds to request packets of a RADIUS authorization through any IPv4 address, which increases system security risks. Therefore, you are advised not to run this command.
- After the **radius-server authorization server-source all-interface** command is run, all the configurations of the **radius-server authorization server-source ip-address** *ip-address* command are cleared.
- If the **radius-server authorization server-source all-interface** command has been configured on the device, the **radius-server authorization server-source ip-address** *ip-address* command configured later does not take effect.

Example

Specify 10.1.1.1 as the IPv4 address used to receive and respond to request packets of a RADIUS authorization server.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization server-source ip-address 10.1.1.1
```

13.2.43 radius-server dead-detect-condition by-server-ip

Function

The **radius-server dead-detect-condition by-server-ip** command configures the device to perform keepalive detection on the RADIUS authentication and accounting servers with the same IP address.

The **undo radius-server dead-detect-condition by-server-ip** command configures the device to perform keepalive detection on only the RADIUS authentication server.

By default, keepalive detection is performed on the RADIUS authentication and accounting servers with the same IP address.

Format

radius-server dead-detect-condition by-server-ip

undo radius-server dead-detect-condition by-server-ip

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device periodically sends authentication request packets to the RADIUS server in Down state. If the RADIUS server responds, the device sets the RADIUS authentication server status to Up. The device does not perform keepalive detection for RADIUS accounting servers in Down state. Instead, the device sets the RADIUS accounting server status to Up only when the server recovery time expires.

To allow the device to promptly detect the status of RADIUS accounting servers that are in Down state, run the **radius-server dead-detect-condition by-server-ip** command. After the command is executed, the device performs keepalive detection on RADIUS servers based on the RADIUS server IP address, so that the status of RADIUS accounting server is associated with the status of authentication server.

Precautions

After the **radius-server dead-detect-condition by-server-ip** command is executed, run the **radius-server testuser** command to configure automatic user detection.

After the **radius-server dead-detect-condition by-server-ip** command is executed, if the authentication and accounting servers sharing the same IP address are in the same VPN instance, the device accumulates the number of authentication and accounting packets sent by the servers. In addition, the status of RADIUS authentication server with the same IP address in the same VPN instance is updated.

Example

Configure the device to perform keepalive detection on the RADIUS authentication and accounting servers with the same IP address.

```
<HUAWEI> system-view
[HUAWEI] radius-server dead-detect-condition by-server-ip
```

13.2.44 radius-server dead-interval dead-count detect-cycle

Function

The **radius-server dead-interval dead-count detect-cycle** command configures the RADIUS server detection interval, number of times the detection interval

cycles, and maximum number of consecutive unacknowledged packets in each detection interval.

The **undo radius-server dead-interval dead-count detect-cycle** command restores the default settings.

By default, the RADIUS server detection interval is 5 seconds, the number of times the detection interval cycles is 2, and the maximum number of consecutive unacknowledged packets in each detection interval is 2.

Format

radius-server { **dead-interval** *dead-interval* | **dead-count** *dead-count* | **detect-cycle** *detect-cycle* }

undo radius-server { **dead-interval** | **dead-count** | **detect-cycle** }

Parameters

Parameter	Description	Value
dead-interval	Specifies the RADIUS server detection interval.	The value is an integer that ranges from 1 to 300, in seconds.
dead-count	Specifies the maximum number of consecutive unacknowledged packets in each detection interval.	The value is an integer that ranges from 1 to 65535.
detect-cycle	Specifies the number of times the detection interval cycles.	The value is an integer that ranges from 1 to 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the system starts, the RADIUS server status detection timer runs. The device sets the RADIUS server status to Up. When the device sends a RADIUS request packet to the RADIUS server, if the conditions for setting the RADIUS server status to Down are met, the device sets the RADIUS server status to Down; if the conditions are not met, the RADIUS server status remains to be Up.

If the device does not receive any response packet from the RADIUS server after sending the first RADIUS Access-Request packet to the server and the condition

that the number of times the device does not receive any response packet from the server (n) is greater than or equal to the maximum number of consecutive unacknowledged packets (*dead-count*) is met in a detection interval, a communication interruption is recorded. If the device still does not receive any response packet from the RADIUS server, the device sets the RADIUS server status to Down when recording the communication interruption for the same times as the detection interval cycles.

Precautions

- If the device has reported a RADIUS server Up alarm and needs to report a RADIUS server Down alarm, the device will send the Down alarm 10 seconds after the Up alarm is sent, even if the RADIUS server Down detection interval is shorter than 10 seconds (for example, the value of *dead-interval* is set to 4 seconds, and the RADIUS server Down detection interval is 8 seconds). This function prevents frequent alarm sending.
- You are advised to set the RADIUS server detection interval, maximum number of consecutive unacknowledged packets in each detection interval, and number of times the detection interval cycles to be greater than the default values on the device to prevent the RADIUS server status from being set to Down.
- To check the RADIUS server status, run the **display radius-server configuration** command. If the RADIUS server status is Down, the device records logs and alarms. For details about logs, see **RDS/4/RDAUTHDOWN**. For details about alarms, see **RDS_1.3.6.1.4.1.2011.5.25.40.15.2.2.1.2 hwRadiusAuthServerDown**.

Example

Set the RADIUS server detection interval to 10 seconds, number of times the detection interval cycles to 2, and maximum number of consecutive unacknowledged packets in each detection interval to 2.

```
<HUAWEI> system-view
[HUAWEI] radius-server dead-interval 10
[HUAWEI] radius-server dead-count 2 [HUAWEI] radius-server detect-cycle 2
```

13.2.45 radius-server detect-server interval

Function

The **radius-server detect-server interval** command configures an automatic detection interval for RADIUS servers in Down status.

The **undo radius-server detect-server interval** command restores the default settings.

The default automatic detection interval is 60 seconds.

Format

radius-server detect-server interval *interval*

undo radius-server detect-server interval

Parameters

Parameter	Description	Value
interval	Specifies the automatic detection interval for RADIUS servers in Down status.	The value is an integer that ranges from 5 to 3600, in seconds.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

After the automatic detection function is enabled using the **radius-server testuser** command, you can run the **radius-server detect-server interval** command to adjust the automatic detection interval for RADIUS servers in Down status.

Example

Set the automatic detection interval for RADIUS servers in Down status to 100 seconds in the RADIUS server template **acs**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server detect-server interval 100
```

13.2.46 radius-server detect-server timeout

Function

The **radius-server detect-server timeout** command configures the timeout period for RADIUS detection packets.

The **undo radius-server detect-server timeout** command restores the default settings.

By default, the timeout period for RADIUS detection packets is 3 seconds.

Format

radius-server detect-server timeout *timeout*

undo radius-server detect-server timeout

Parameters

Parameter	Description	Value
timeout	Specifies the timeout period for RADIUS detection packets.	The value is an integer that ranges from 1 to 10, in seconds.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the automatic detection function is enabled using the **radius-server testuser** command and the device sends detection packets to the RADIUS server, the device determines whether to switch the RADIUS server status based on whether it receives response packets from the RADIUS server within the timeout period. The following table lists the switchover conditions.

After the automatic detection function is enabled, automatic detection is classified into the following conditions depending on differences of the RADIUS server status.

Server Status	Whether Automatic Detection Is Supported	Time When an Automatic Detection Packet Is Sent	Condition for Switching the Server Status
Down	Automatic detection is supported by default.	An automatic detection packet is sent after the automatic detection period expires.	If the device receives a response packet from the RADIUS server within the timeout period for detection packets, the device marks the RADIUS server status as Up; otherwise, the RADIUS server status remains Down.

Server Status	Whether Automatic Detection Is Supported	Time When an Automatic Detection Packet Is Sent	Condition for Switching the Server Status
Up	Automatic detection can be enabled using the **radius-server detect-server up-server interval** command.	An automatic detection packet is sent after the automatic detection period expires.	If the conditions for marking the RADIUS server status as Down are met, the device marks the RADIUS server status as Down; otherwise, the RADIUS server status remains Up.
Force-up	Automatic detection is supported by default.	An automatic detection packet is sent immediately.	If the device receives a packet from the RADIUS server within the timeout period, the device marks the RADIUS server status as Up; otherwise, the device marks the RADIUS server status as Down.

NOTE

On a large-scale network, you are advised not to enable automatic detection for RADIUS servers in Up state. This is because if automatic detection is enabled on multiple NAS devices, the RADIUS server periodically receives a large number of detection packets when processing RADIUS Access-Request packets source from users, which may deteriorate processing performance of the RADIUS server.

After the **radius-server testuser** command is configured, the dead-time timer configured using the **radius-server dead-time** command does not take effect.

Precautions

You can run the **radius-server detect-server timeout** command to adjust the timeout period for RADIUS detection packets based on the actual response rate of the RADIUS server. You are advised to set a timeout period for RADIUS detection packets smaller than the automatic detection interval to prevent the device from sending a detection packet again before completing processing the response packet from the RADIUS server. If the configured timeout period for RADIUS detection packets is longer than the automatic detection interval, the smaller value of the two is used as the timeout period.

- For the RADIUS server in Down state, the smaller one between the values configured using the **radius-server detect-server timeout** and **radius-server detect-server interval** commands is the timeout period for detection packets.
- For the RADIUS server in Up state, the smaller one between the values configured using the **radius-server detect-server timeout** and **radius-server detect-server up-server interval** command is the timeout period for detection packets.

Example

Set the timeout period for RADIUS detection packets to 5 seconds in the RADIUS server template **acs**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server detect-server timeout 5
```

13.2.47 radius-server detect-server up-server interval

Function

The **radius-server detect-server up-server interval** command enables automatic detection for RADIUS servers in Up status and configures the automatic detection interval.

The **undo radius-server detect-server up-server interval** command restores the default settings.

By default, a device does not automatically detect RADIUS servers in Up status.

Format

radius-server detect-server up-server interval *interval*

undo radius-server detect-server up-server interval

Parameters

Parameter	Description	Value
interval	Specifies the automatic detection interval for RADIUS servers in Up status.	The value is an integer that ranges from 0 or 2 to 3600, in seconds. The value 0 indicates that the device does not automatically detect RADIUS servers in Up status.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After automatic detection is enabled using the **radius-server testuser** command, the device automatically detects only RADIUS servers in Down status by default.

To make the device automatically detect RADIUS servers in Up status, run the **radius-server detect-server up-server interval** command to enable automatic detection for RADIUS servers in Up status and configure the automatic detection interval.

Precautions

On a large-scale network, you are advised not to enable automatic detection for RADIUS servers in Up state. This is because if automatic detection is enabled on multiple NAS devices, the RADIUS server periodically receives a large number of detection packets when processing RADIUS Access-Request packets source from users, which may deteriorate processing performance of the RADIUS server.

Example

Enable automatic detection for RADIUS servers in Up status and set the automatic detection interval to 100 seconds in the RADIUS server template **acs**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server detect-server up-server interval 100
```

13.2.48 radius-server dead-time

Function

The **radius-server retransmit timeout dead-time** command sets the number of times that RADIUS request packets are interval for the server to revert to the active status.

The **undo radius-server retransmit timeout dead-time** command restores the default interval for the server to revert to the active status.

By default, the interval for the server to revert to the active status is 5 minutes.

Format

radius-server dead-time *dead-time*

undo radius-server dead-time [*dead-time*]

Parameters

Parameter	Description	Value
dead-time	Specifies the interval for the server to revert to the active status.	The value is an integer that ranges from 1 to 65535, in minutes.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **radius-server dead-time** *dead-time* command to configure the duration for which the RADIUS server remains Down. After the device sets the RADIUS server status to Down and the interval specified by *dead-time* expires, the device resets the server status to Force-up. Servers in Force-up and Up states have the same priority and participate in RADIUS server selection based on the algorithm specified by **radius-server algorithm**. If a new user needs to be authenticated in RADIUS mode and no RADIUS server is available, the device attempts to re-establish a connection with a RADIUS server in Force-up status. The Force-up status is defined to prevent servers in Down status from remaining idle.

NOTE

After the **radius-server testuser** command is configured, the dead-time timer configured using the **radius-server dead-time** command does not take effect.

This command can improve the reliability of RADIUS authentication.

Example

Set the interval for the server to revert to the active status to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server dead-time 10
```

13.2.49 radius-server encapsulation ipv4 traffic-statistics enable

Function

The **radius-server encapsulation ipv4 traffic-statistics enable** command enables a device to encapsulate the standard RADIUS attributes 42, 43, 47, 48, 52, and 53 only into IPv4 traffic.

The **undo radius-server encapsulation ipv4 traffic-statistics enable** command restores the default configuration.

By default, a device encapsulates both IPv4 and IPv6 traffic with the standard RADIUS attributes 42, 43, 47, 48, 52, and 53.

Format

radius-server encapsulation ipv4 traffic-statistics enable

undo radius-server encapsulation ipv4 traffic-statistics enable

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

After this command is run, the device encapsulates the standard RADIUS attributes 42, 43, 47, 48, 52, and 53 only into IPv4 traffic. If the **accounting dual-stack separate** command is run to enable separate traffic statistics collection or rate limiting for IPv4 and IPv6 users, the device encapsulates IPv6 traffic with the Huawei proprietary attributes 26-166, 26-167, 26-168, 26-169, 26-170, and 26-171.

Example

In the RADIUS server template **acs**, enable the function of encapsulating the standard RADIUS attributes 42, 43, 47, 48, 52, and 53 only into IPv4 traffic.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server encapsulation ipv4 traffic-statistics enable
Warning: This operation may cause online users' traffic statistics inaccurate, Re-online is recommended after this operation, continue?[Y/N]y
```

13.2.50 radius-server format-attribute

Function

The **radius-server format-attribute** command configures the format of the NAS-Port attribute.

The **undo radius-server format-attribute** command deletes the configured attribute format.

By default, the format of the NAS-Port attribute is **new**.

Format

radius-server format-attribute nas-port *nas-port-sting* [**decimal**]

undo radius-server format-attribute nas-port

Parameters

Parameter	Description	Value
nas-port *nas-port-sting*	Specifies the format of the NAS-Port attribute. In the *nas-port-string* parameter in binary format: ● The keywords **s**, **t**, **p**, **o**, and **i** indicate slot, subslot, port, out-vlan (qinqvlan)/vpi, and vlan (user-vlan)/vci respectively. The keywords **n** and **z** are used as paddings. The keyword **n** indicates 1 and the keyword **z** indicates 0. ● The keywords **s**, **t**, **p**, **o**, and **i** must be followed by numbers, and the numbers must range from 1 to 32. The keywords **s**, **t**, **p**, **o**, and **i** can appear in the format string only once. ● The keywords **s**, **t**, **p**, **o**, **i**, **n**, and **z** must range from 1 to 9. ● **n** and **z** can appear multiple times at any position. They are followed by numbers. For example, **n12** indicates that this position is filled in with twelve 1s, and **z12** indicates that this position is filled in with twelve 0s. ● The character string must contain 32 bits. ● The format string must start with **s**, **t**, **p**, **o**, **i**, **n**, or **z** and end with a number.	The value is a character string. When the *nas-port-string* parameter is in binary format, the value is a string of 1 to 32 characters. When the *nas-port-string* parameter is in decimal format, the value is a string of 1 to 9 characters.

Parameter	Description	Value
	• If no VLAN exists, you can add **n** or **z** before **o** or **i** to indicate whether this position is filled in with 0s or 1s. That is, **n** and **z** can be followed by numbers, **o**, or **i** in this case, and the numbers must range from 1 to 32. • To specify the format string, determine the interface type, and then determine the encapsulation type of the interface. If the format string does not contain **o** or **i**, the NAS-Port attribute does not contain the QinQ VLAN or user VLAN field. If the format string contains **o** or **i** but no outer VLAN exists, the outer VLAN field is filled in with 0s. If **n** is added before **o** or **i**, this field is filled in with 1s when no outer VLAN or inner VLAN exists. In the *nas-port-string* parameter in decimal format: • The keywords **s**, **t**, **p**, **o**, and **i** indicate slot, subslot, port, out-vlan (qinqvlan)/vpi, and vlan (user-vlan)/vci respectively. • The keywords **s**, **t**, **p**, **o**, and **i** must be followed by a number ranging from 1 to 9. Each keyword can appear only once. • If **s**, **t**, **p**, **o**, and **i** is followed by a number,	

Parameter	Description	Value
	the first number must range from 1 to 9 and cannot be 0. • The string can contain at most 9 digits. • The string must start with **s**, **t**, **p**, **o**, or **i** and end with a number. • If no VLAN exists, this field is filled in with 0. In the decimal string, this field cannot be filled in with 1. • To specify the format string, determine the interface type, and then determine the encapsulation type of the interface. If the format string does not contain **o** or **i**, the NAS-Port attribute does not contain the QinQ VLAN or user VLAN field. If the format string contains **o** or **i** but no outer VLAN exists, the outer VLAN field is filled in with 0 by default. If no VLAN exists, both the inner and outer VLAN fields are filled in with 0 by default.	
decimal	Indicates that *nas-port-string* is in decimal format. If this parameter is not specified, *nas-port-string* is in binary format.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The NAS port format affects the information about the physical port. The NAS port format can be used by the RADIUS server to process services, such as binding the user name and port. This attribute is developed by Huawei, which is used to ensure connectivity and service cooperation among Huawei devices.

If the **radius-server nas-port-format** command sets the format of the NAS-Port attribute to **new** (the default format is **new**), the device will check whether the **radius-server format-attribute nas-port** command configuration exists. If so, the device will assemble the NAS-Port attribute in the format configured by the **radius-server format-attribute nas-port** command. If no, the device will assemble the NAS-Port attribute in the **new** format. If the **radius-server nas-port-format** command sets the format of the NAS-Port attribute to **old**, the device will assemble the NAS-Port attribute in the **old** format, regardless of whether the **radius-server format-attribute nas-port** command configuration exists.

Example

Configure the format of the NAS-Port attribute to s2t2p6no10ni12 in binary format. That is, the NAS-Port attribute consists of a 2-bit slot field, a 2-bit subslot field, a 6-bit port field, a 10-bit outer VLAN field, and a 12-bit inner VLAN field. If the outer VLAN does not exist, this field is filled in with ten 1s. If the inner VLAN does not exist, this field is filled in with twelve 1s. Therefore, the NAS-port attribute contains 32 bits.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server format-attribute nas-port s2t2p6no10ni12
```

Configure the format of the NAS-Port attribute to s1t1p2o1i1 in decimal format. That is, the NAS-Port attribute consists of a 1-bit slot field, a 1-bit subslot field, a 2-bit port field, a 1-bit outer VLAN field, and a 1-bit inner VLAN field. If the outer VLAN does not exist, this field is filled in with 0. If the inner VLAN does not exist, this field is filled in with 0.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server format-attribute nas-port s1t1p2o1i1 decimal
```

13.2.51 radius-server framed-ip-address no-user-ip enable

Function

The **radius-server framed-ip-address no-user-ip enable** command enables the device to encapsulate the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address.

The **undo radius-server framed-ip-address no-user-ip enable** command disables the device from encapsulating the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address.

By default, the device does not encapsulate the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address.

Format

radius-server framed-ip-address no-user-ip enable

undo radius-server framed-ip-address no-user-ip enable

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

In MAC address authentication triggered through DHCP packets, a user can obtain an IP address only after being successfully authenticated. The RADIUS authentication request packet sent by the user does not carry the IP address of the user. By default, the device does not encapsulate the RADIUS attribute Framed-IP-Address into the RADIUS authentication request packet sent by the user when forwarding the packet. If the RADIUS server connected to the device requires that the received RADIUS authentication request packets contain the RADIUS attribute Framed-IP-Address, run the **radius-server framed-ip-address no-user-ip enable** command. Then the device uses the IP address 0.0.0.0 to encapsulate the RADIUS attribute Framed-IP-Address when receiving the RADIUS authentication request packets that do not contain the user IP address.

Example

Enable the device to encapsulate the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server framed-ip-address no-user-ip enable
```

13.2.52 radius-server hw-ap-info-format include-ap-ip

Function

The **radius-server hw-ap-info-format include-ap-ip** command configures the AP's IP address carried in Huawei extended attribute HW-AP-Information.

The **undo radius-server hw-ap-info-format** command restores the default setting.

By default, Huawei extended attribute HW-AP-Information does not carry AP's IP address.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

radius-server hw-ap-info-format include-ap-ip

undo radius-server hw-ap-info-format

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

RADIUS is a fully extensible protocol. Device vendors can expand the No. 26 attribute defined in the protocol to implement functions not supported by standard RADIUS attributes. Huawei defines the No. 141 sub-attribute (HW-AP-Information) in the No. 26 attribute to indicate AP information, including the MAC and IP addresses of an AP. The HW-AP-Information attribute is carried in the authentication or accounting request packet send by a device, so that the RADIUS server can use the AP's MAC and IP addresses as the filter criterion to select a policy template to be delivered.

When an AP's IP address is carried in the HW-AP-Information attribute, the encapsulation format of the attribute is AP-MAC AP-IP.

Example

#Configure the AP's IP address in Huawei extended attribute HW-AP-Information.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] radius-server hw-ap-info-format include-ap-ip
```

13.2.53 radius-server hw-dhcp-option-format

Function

The **radius-server hw-dhcp-option-format** command sets the format of the Huawei extended attribute HW-DHCP-Option.

The **undo radius-server hw-dhcp-option-format** command restores the default setting.

By default, the format of HW-DHCP-Option is old.

Format

radius-server hw-dhcp-option-format { **new** | **old** }

undo radius-server hw-dhcp-option-format

Parameters

Parameter	Description	Value
new	Sets the format of Huawei extended attribute HW-DHCP-Option to new.	-
old	Sets the format of Huawei extended attribute HW-DHCP-Option to old.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The RADIUS protocol has good extensibility. Device vendors can expand the No. 26 RADIUS attribute to implement new functions. Huawei defines that the No.158 sub-attribute in the No.26 attribute represents DHCP option and is encapsulated through Type, Length, Value (TLV). The device adds this attribute in authentication request or accounting request packets and sends the DHCP option information to the RADIUS server.

To connect to different types of RADIUS server, the device supports two HW-DHCP-Option formats: **new** and **old**.

- **new**: When the attribute is encapsulated through TLV, the Type field length is 1 byte. This format is applicable when the device connects to most types of RADIUS servers.
- **old**: When the attribute is encapsulated through TLV, the Type field length is 2 bytes. This format is applicable when the device connects to special RADIUS servers, for example, Huawei RADIUS server.

Example

Set the format of Huawei extended attribute HW-DHCP-Option to new.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] radius-server hw-dhcp-option-format new
```


13.2.54 radius-server nas-identifier-format

Function

The **radius-server nas-identifier-format** command sets the encapsulation format of the NAS-Identifier attribute.

The **undo radius-server nas-identifier-format** command restores the default encapsulation format of the NAS-Identifier attribute.

By default, the NAS-Identifier attribute encapsulation format is the NAS device's hostname.

Format

radius-server nas-identifier-format { **hostname** | **vlan-id** | **ap-info** }

undo radius-server nas-identifier-format

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **ap-info** parameter.

Parameters

Parameter	Description	Value
hostname	Sets the encapsulation format of NAS-Identifier to the NAS device's host name.	-
vlan-id	Sets the encapsulation format of NAS-Identifier to a user's VLAN ID.	-
ap-info	Sets the encapsulation format of NAS-Identifier to the AP's MAC address.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

A RADIUS server uses the NAS-Identifier attributes to identify NASs. The NASs also use the NAS-Identifier attributes carried in the sent RADIUS packets to identify themselves.

When the RADIUS server interconnected with the device requires that the NAS-Identifier attribute value is the MAC address of the AP when the device functions as an AC in a wireless scenario, you need to run the **radius-server nas-identifier-format ap-info** command.

Example

Set the NAS-Identifier encapsulation format to VLAN ID.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server nas-identifier-format vlan-id
```

13.2.55 radius-server nas-port-format

Function

The **radius-server nas-port-format** command sets the format of the NAS port attribute.

The **undo radius-server nas-port-format** command restores the default format of the NAS port attribute.

By default, the new NAS port format is used.

Format

radius-server nas-port-format { **new** | **old** }

undo radius-server nas-port-format

Parameters

Parameter	Description	Value
new	Uses the new format of an NAS port. The new format of the NAS port attribute is slot number (8 bits) + subslot number (4 bits) + port number (8 bits) + VLAN ID (12 bits).	-

Parameter	Description	Value
old	Uses the old format of an NAS port. The old format of the NAS port attribute is slot number (12 bits) + port number (8 bits) + VLAN ID (12 bits).	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NAS port format affects the information about the physical port. The NAS port format can be used by the RADIUS server to process services, such as binding the user name and port. This attribute is developed by Huawei, which is used to ensure connectivity and service cooperation among Huawei devices.

Precautions

The difference between the two NAS port formats lies in the physical ports connected to Ethernet access users.

- The new format of the NAS port attribute is slot number (8 bits) + subslot number (4 bits) + port number (8 bits) + VLAN ID (12 bits).
- The old format of the NAS port attribute is slot number (12 bits) + port number (8 bits) + VLAN ID (12 bits).

The format of the NAS port attribute for Asymmetric Digital Subscriber Line (ADSL) access users is slot number (4 bits) + subslot number (2 bits) + port number (2 bits) + VPI (8 bits) + VCI (16 bits). This format is not affected by the command.

Example

Set the format of the NAS port attribute to **new**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server nas-port-format new
```


13.2.56 radius-server nas-port-id-format

Function

The **radius-server nas-port-id-format** command sets the format of the NAS port ID attribute.

The **undo radius-server nas-port-id-format** command restores the default format of the NAS port ID attribute.

By default, the new format of the NAS port ID attribute is used.

Format

radius-server nas-port-id-format { **new** [**client-option82**] | **old** | **vendor** *vendor-id* }

undo radius-server nas-port-id-format

Parameters

Parameter	Description	Value
new	Uses the new format of the NAS port ID.	-
client-option82	Uses the content of the Option82 field as the format of the NAS-Port-Id attribute.	-
old	Uses the old format of the NAS port ID.	-
vendor *vendor-id*	Uses the NAS port ID format that is customized by the vendor.	The value is an integer. Currently, the value can only be 9.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NAS port format and the NAS port ID format are developed by Huawei, which are used to ensure connectivity and service cooperation among Huawei devices.

Precautions

Port of the NAS that is authenticating the user. The NAS-Port-Id attribute has the following formats:

- New:

  For Ethernet access users, the NAS-Port-Id is in the format "slot=xx; subslot=xx; port=xxx; vlanid=xxxx; interfaceName=*port*", in which "slot" is 64 or ranges from 0 to 15, "subslot" ranges from 0 to 15, "port" ranges from 0 to 255, "vlanid" ranges from 1 to 4094, "interfaceName" indicates the user access interface, including the interface type and number.

  For ADSL access users, the NAS-Port-Id is in the format "slot=xx; subslot=x; port=x; VPI=xxx; VCI=xxxxx; interfaceName=*port*", in which "slot" ranges from 0 to 15, "subslot" 0 to 9, "port" 0 to 9, "VPI" 0 to 255, and "VCI" 0 to 65535, "interfaceName" indicates the user access interface, including the interface type and number.

- New client-option82:

  When a PPPoE or DHCP user goes online, if the PPPoE or DHCP packet sent by the user contains the Option 82 field, the device encapsulates the content of the circuit ID suboption in the Option 82 field into the NAS-Port-Id (87) attribute of a RADIUS packet, and then sends the RADIUS packet to the RADIUS server, binding the user account to the access location and preventing an account from being shared by multiple users. In this case, the format of NAS-Port-Id (87) attribute in the RADIUS packet is the same as that of the circuit ID suboption in the Option 82 field. To configure the format of the circuit ID suboption, run the **dhcp option82 format** or **pppoe intermediate-agent information format** command.

  NOTE

  - If the PPPoE or DHCP packet does not contain the Option 82 field, the format of the NAS-Port-Id (87) attribute in the RADIUS packet is **new**.
  - If the **new client-option82** parameter is selected, the device encapsulates the content of the first 128 bytes in the Circuit ID suboption of the Option 82 field into the NAS-Port-Id (87) attribute of a RADIUS packet. If the first 128 bytes contain 0, the device only encapsulates bytes before the first 0. If the first byte of the Circuit ID value is 0 or no Circuit ID value exists, the format of the NAS-Port-Id (87) attribute in RADIUS packets is **new**.

- Old:

  For Ethernet access users, the NAS-Port-Id is in the format "port number (2 characters) + sub-slot ID (2 bytes) + card number (3 bytes) + VLAN ID (9 characters)."

  For ADSL access users: port number (2 characters) + sub-slot ID (2 bytes) + card number (3 bytes) + VPI (8 characters) + VCI (16 characters). The fields are prefixed with 0s if they contain fewer bytes than specified.

- vendor *vendor-id*:

  The NAS port ID format is customized by the vendor. The value of *vendor-id* currently can only be 9. It is in the format of interface type+interface number, indicating a user access interface. To check the access interface of a specified user, run the **display access-user user-id** *user-id* command. In the command output, the **User access Interface** field indicates the access interface of a user.

NOTE

If this attribute carries Chinese characters, it cannot be delivered using the **radius-attribute set** *attribute-name attribute-value* command.

Example

Set the format of the NAS port ID attribute to **new**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server nas-port-id-format new
```

13.2.57 radius-server retransmit timeout

Function

The **radius-server retransmit timeout** command sets the number of times that RADIUS request packets are retransmitted, timeout period.

The **undo radius-server retransmit timeout** command restores the default number of retransmission times, the default timeout period.

By default, the number of retransmission times is 5, timeout period is 2 seconds.

Format

radius-server { **retransmit** *retry-times* | **timeout** *time-value* } *

undo radius-server { **retransmit** [*retry-times*] | **timeout** [*time-value*] } *

Parameters

Parameter	Description	Value
retransmit *retry-times*	Specifies the number of retransmission times. The value is the total number of times a packet is transmitted.	The value is an integer that ranges from 1 to 5.
timeout *time-value*	Specifies the timeout period.	The value is an integer that ranges from 1 to 100, in seconds.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The retransmission upon timeout mechanism is configured for a device to forward RADIUS Access-Request packets sourced from users to the server. The overall retransmission time depends on the retransmission interval, retransmission times, RADIUS server status, and number of servers configured in the RADIUS server template.

You can configure the number of times that RADIUS request packets are retransmitted and the timeout period using the **radius-server retransmit** *retry-times* and **radius-server timeout** *time-value* commands, respectively. If a device sends an authentication request packet to the RADIUS server and does not receive any response packet from the server during the timeout period, the device sends an authentication request packet again.

This command can improve the reliability of RADIUS authentication.

Precautions

- The request packet retransmission time (number of retransmission times x timeout period) of the RADIUS server must be shorter than the request packet retransmission time of the Portal server.
- If more than 8 authentication server IP addresses are configured in the RADIUS server template, reduce the number of retransmission times and timeout period.

Example

Set the number of retransmission times to 3, the timeout period to 2s.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server retransmit 3 timeout 2
```

13.2.58 radius-server session-manage

Function

The **radius-server session-manage** command enables session management on the RADIUS server.

The **undo radius-server session-manage** command disables session management on the RADIUS server.

By default, session management is disabled on the RADIUS server.

Format

radius-server session-manage { *ip-address* [**vpn-instance** *vpn-instance-name*] **shared-key cipher** *share-key* | **any** }

undo radius-server session-manage [*ip-address* [**vpn-instance** *vpn-instance-name*] | **all**]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the RADIUS session management server.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance bound to the RADIUS session management server.	The value must be the name of an existing VPN instance.
shared-key cipher *share-key*	Specifies the shared key of the RADIUS session management server.	The value is a string of case-sensitive characters that cannot contain spaces and question marks. *share-key* can be a string of 1-128 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.
any	Indicates that no RADIUS session management server is specified.	-
all	Deletes all RADIUS session management servers.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve device security, run this command to enable session management on the RADIUS server. After this function is enabled, the device checks the source IP addresses and shared keys for the received session management packets. When the source IP addresses and shared keys match the configured values, the packets are processed; otherwise, the packets are discarded.

Precautions

- This command has been supported since V200R010C00. When a device is upgraded from a version earlier than V200R010C00 to V200R010C00 or a later version, the **radius-server session-manage any** command is configured by default.
- When the **any** parameter is specified, there is a security risk. You are advised to configure the IP address and shared key for a specified RADIUS session management server.
- In V200R020C10SPC100 and later versions, you also need to run the **radius-server session-manage server-source** command to configure an IPv4 address for receiving and responding to request packets of a RADIUS session management server so that the session management function of the RADIUS server can take effect.

Example

Enable session management on the RADIUS server, and set the IP address and shared key of the RADIUS session management server to 10.1.1.1 and **YsHsjx_202206** respectively.

```
<HUAWEI> system-view
[HUAWEI] radius-server session-manage 10.1.1.1 shared-key cipher YsHsjx_202206
```

13.2.59 radius-server session-manage server-source

Function

The **radius-server session-manage server-source** command configures an IPv4 address for receiving and responding to request packets of a RADIUS session management server.

The **undo radius-server session-manage server-source** command restores the default setting.

By default, the device does not receive or respond to any request packet of a RADIUS session management server.

Format

radius-server session-manage server-source { **ip-address** *ip-address* | **all-interface** }

undo radius-server session-manage server-source { **ip-address** { *ip-address* | **all** } | **all-interface** }

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation. The value range depends on the device types.

Parameter	Description	Value
all-interface	Specifies the IPv4 address as 0.0.0.0. That is, the device receives and responds to request packets of a RADIUS session management server through any IPv4 address.	-
all	Indicates all IPv4 addresses specified by **ip-address** *ip-address*.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no IPv4 address can be used to receive or respond to request packets of a RADIUS session management server. When the device needs to establish a connection with a RADIUS session management server, you can run this command to specify an IPv4 address for receiving and responding to request packets of the RADIUS session management server.

Precautions

- After you run this command to configure an IPv4 address for the device to receive and respond to request packets of a RADIUS session management server, the RADIUS session management server can communicate with the device only through this IPv4 address. Ensure that the RADIUS session management server can communicate with the device through this IPv4 address at Layer 3.
- After the **radius-server session-manage server-source all-interface** command is run, the device receives and responds to request packets of a RADIUS session management through any IPv4 address, which increases system security risks. Therefore, you are advised not to run this command.
- After the **radius-server session-manage server-source all-interface** command is run, all the configurations of the **radius-server session-manage server-source ip-address** *ip-address* command are cleared.
- If the **radius-server session-manage server-source all-interface** command has been configured on the device, the **radius-server session-manage server-source ip-address** *ip-address* command configured later cannot be delivered.

- If the device is upgraded from a version earlier than V200R020C10SPC100 and the session management function is enabled for the RADIUS server, the device delivers the **radius-server session-manage server-source all-interface** command by default to enable the session management function for the RADIUS server with an all-zero address.
- In versions earlier than V200R020C10SPC100, if the session management function of the RADIUS server is enabled, you need to enable the session management function when using the session management function of the RADIUS server in versions later than V200R020C10SPC100. That is, run the **radius-server session-manage server-source all-interface** command to enable the session management function of the RADIUS server with an all-zero IP address or run the **radius-server session-manage server-source ip-address** *ip-address* command to enable the session management function of the RADIUS server with a specified IP address.
- In V200R020C10SPC100 and later versions, you also need to run the **radius-server session-manage server-source** command to configure an IPv4 address for receiving and responding to request packets of a RADIUS session management server so that the session management function of the RADIUS server can take effect.

Example

Specify 10.1.1.1 as the IPv4 address used to receive and respond to request packets of a RADIUS session management server.

```
<HUAWEI> system-view
[HUAWEI] radius-server session-manage server-source ip-address 10.1.1.1
```

13.2.60 radius-server shared-key (RADIUS server template view)

Function

The **radius-server shared-key** command configures the shared key of a RADIUS server.

The **undo radius-server shared-key** command deletes the shared key of a RADIUS server.

By default, no shared key of RADIUS server is configured.

Format

radius-server shared-key cipher *key-string*

undo radius-server shared-key

Parameters

Parameter	Description	Value
cipher	Indicates the shared key in cipher text.	-

Parameter	Description	Value
key-string	Specifies the shared key of a RADIUS server.	The value is a case-sensitive character string without spaces, single quotation marks ('), or question marks (?). *key-string* can be a string of 1-128 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with a RADIUS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. To ensure validity of both communication parties, the device and RADIUS server must be configured with the same shared key.

Precautions

For security purposes, change the default shared key immediately. It is recommended that the new shared key contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

Example

Set the shared key of a RADIUS server to **YsHsjx_202206** in cipher text.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server shared-key cipher YsHsjx_202206
```


13.2.61 radius-server shared-key (system view)

Function

The **radius-server shared-key** command configures the shared key of a RADIUS server.

The **undo radius-server shared-key** command deletes the shared key of a RADIUS server.

By default, no global shared key is configured for the RADIUS server.

Format

radius-server ip-address { *ipv4-address* | *ipv6-address* } **shared-key cipher** *key-string*

undo radius-server ip-address { *ipv4-address* | *ipv6-address* } **shared-key**

Parameters

Parameter	Description	Value
ip-address { *ipv4-address* | *ipv6-address* }	Specifies the IPv4 or IPv6 address of the RADIUS server.	• *ipv4-address*: The value is in dotted decimal notation. • *ipv6-address*: The value is a 32-bit hexadecimal string in format X:X:X:X:X:X:X:X.
cipher *key-string*	Specifies the shared key in cipher text.	The value is a case-sensitive character string without spaces, single quotation marks ('), or question marks (?). *key-string* can be a string of 1-128 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with a RADIUS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. To ensure validity of both communication parties, the device and RADIUS server must be configured with the same shared key.

You can run the **radius-server shared-key** command in the RADIUS server template view to configure the shared keys. However, after this command is run, all RADIUS servers in the template use the same shared key. To configure different shared keys for RADIUS servers, run the **radius-server shared-key** command in the system view.

Precautions

To improve security, it is recommended that the shared key contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

When the shared keys are configured in both the RADIUS server template and system view, the configuration in the system view takes effect.

Example

Set the shared key for RADIUS server to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] radius-server ip-address 10.1.1.1 shared-key cipher YsHsjx_202206
```

13.2.62 radius-server support chargeable-user-identity

Function

The **radius-server support chargeable-user-identity** command configures a device to support the CUI attribute.

The **undo radius-server support chargeable-user-identity** command restores the default settings.

By default, a device does not support the CUI attribute.

Format

radius-server support chargeable-user-identity [**not-reject**]

undo radius-server support chargeable-user-identity

Parameters

Parameter	Description	Value
not-reject	Configures the device not to process the CUI attribute.	-

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

In a scenario where roaming accounting is performed on a carrier network, the same user may have register different user names in different network environments. Therefore, the user name cannot be used as the unique ID for accounting. In this case, you can use the RADIUS Chargeable-User-Identity (CUI) attribute defined in the RFC to resolve this issue. RADIUS authentication servers can provide users with unique CUI attribute values that function as the users' accounting IDs.

By default, RADIUS Access-Request packets sent by a device do not carry the CUI attribute. If Access-Accept packets responded by the RADIUS server carry the CUI attribute, the device retains this attribute in the Accounting-Request(Start), Accounting-Request(Interim-update), and Accounting-Request(Stop) packets without any processing.

After the **radius-server support chargeable-user-identity** [**not-reject**] command is configured, the RADIUS Access-Request packets sent by the device carry the CUI attribute and the attribute value is Null.

- If Access-Accept packets responded by the RADIUS server carry the CUI attribute, the device retains this attribute in the Accounting-Request(Start), Accounting-Request(Interim-update), and Accounting-Request(Stop) packets without any processing; the previously delivered CUI attribute is carried in the Access-Request packets triggered by the subsequent reauthentication, authentication coverage, and roaming for users.
- If Access-Accept packets responded by the RADIUS server does not carry the CUI attribute or carry the CUI attribute whose value is Null:
  - If the **not-reject** parameter is not specified, user authentication fails.
  - If the **not-reject** parameter is specified, the device ignores the CUI attribute and user authentication succeeds.

Example

Configure a device to support the CUI attribute.


```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server support chargeable-user-identity
```

13.2.63 radius-server template

Function

The **radius-server template** command creates a RADIUS server template and displays the RADIUS server template view.

The **undo radius-server template** command deletes a RADIUS server template.

By default, the device contains the RADIUS server template **default**. The template can be modified, but cannot be deleted.

Format

radius-server template *template-name*

undo radius-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of a RADIUS server template.	The value is a string of 1 to 32 case-sensitive characters, including letters (case-sensitive), numerals (0 to 9), periods (.), hyphens (-), and underscores (_). The value cannot be - or --.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Creating a RADIUS server template is the prerequisite for configuring RADIUS authentication and accounting. You can perform RADIUS configurations, such as the configuration of authentication servers, accounting servers, and shared key only after a RADIUS server template is created.

Follow-up Procedure

Configure an authentication server, an accounting server, and shared key in the RADIUS server template view, and then run the **radius-server** command to apply the RADIUS server template.

Example

Create a RADIUS server template **template1** and enter the RADIUS server template view.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1]
```

13.2.64 radius-server testuser

Function

The **radius-server testuser** command enables the automatic detection function and configures an automatic detection account.

The **undo radius-server testuser** command restores the default settings.

By default, the automatic detection function is disabled.

Format

radius-server testuser username *user-name* **password cipher** *password*

undo radius-server testuser

Parameters

Parameter	Description	Value
username *user-name*	Specifies a user name used for automatic detection.	The value is a string of 1 to 253 case-sensitive characters. If the user name contains spaces, you must enclose the name with double quotation marks ("), for example, "user for test".
password cipher *password*	Specifies the user password for automatic detection.	The value is a character string of 1 to 128 characters without spaces and question marks. It is case sensitive. If it is in cipher text, the password is a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

After the RADIUS server status is set to Down, you can configure the automatic detection function to test the RADIUS server reachability.

For the automatic status detection function, only the automatic detection user name and password need to be configured in the RADIUS server template on the device, and the automatic detection account does not need to be configured on the RADIUS server. Authentication success is not mandatory. If the device can receive the authentication failure response packet, the RADIUS server is properly working.

On a large-scale network, you are advised not to enable automatic detection for RADIUS servers in Up state. This is because if automatic detection is enabled on multiple NAS devices, the RADIUS server periodically receives a large number of detection packets when processing RADIUS Access-Request packets source from users, which may deteriorate processing performance of the RADIUS server.

You can run the **radius-server detect-server timeout** command to configure the timeout period for detection packets.

Example

Create a user account with the user name **test** and password **YsHsjx_202206** in RADIUS server template **acs**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server testuser username test password cipher YsHsjx_202206
```

13.2.65 radius-server traffic-unit

Function

The **radius-server traffic-unit** command sets the traffic unit used by a RADIUS server.

The **undo radius-server traffic-unit** command restores the default traffic unit used by a RADIUS server.

The default RADIUS traffic unit is byte on the device.

Format

radius-server traffic-unit { **byte** | **kbyte** | **mbyte** | **gbyte** }

undo radius-server traffic-unit

Parameters

Parameter	Description	Value
byte	Indicates that the traffic unit is byte.	-
kbyte	Indicates that the traffic unit is kilobyte.	-
mbyte	Indicates that the traffic unit is megabyte.	-
gbyte	Indicates that the traffic unit is gigabyte.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Different RADIUS servers may use different traffic units; therefore, you need to set the traffic unit for each RADIUS server group on the router and the traffic unit must be the same as that on the RADIUS server.

Example

Set the traffic unit used by a RADIUS server to kilobyte.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server traffic-unit kbyte
```

13.2.66 radius-server user-name domain-included

Function

The **radius-server user-name domain-included** command configures the device to encapsulate the domain name in the user name in the packets sent to a RADIUS server.

The **radius-server user-name original** command configures the device not to modify the user name entered by the user in the packets sent to a RADIUS server.

The **undo radius-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name in the packets sent to a RADIUS server.

The **undo radius-server user-name domain-included except-eap** command configures the device not to encapsulate the domain name in the user name in

the packets sent to a RADIUS server (applicable to authentication modes except EAP authentication).

By default, the device does not modify the user name entered by the user in the packets sent to a RADIUS server.

Format

radius-server user-name domain-included

radius-server user-name original

undo radius-server user-name domain-included

undo radius-server user-name domain-included except-eap

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The format of a user name is user name@domain name. In the user name, @ is the domain name delimiter. The domain name delimiter can also be any of the following symbols: \ / : < > | ' %.

If the RADIUS server does not accept the user name with the domain name, run the **undo radius-server user-name domain-included** command to delete the domain name from the user name.

Precautions

If the user names in the RADIUS packets sent from the device to RADIUS server contain domain names, ensure that the total length of a user name (user name + domain name delimiter + domain name) is not longer than 253 characters; otherwise, the user name cannot be contained in RADIUS packets. As a result, authentication will fail.

Example

Configure the device not to encapsulate the domain name in the user name in the packets sent to a RADIUS server.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] undo radius-server user-name domain-included
```


13.2.67 reset radius-server accounting-stop-packet

Function

The **reset radius-server accounting-stop-packet** command clears statistics on the remaining buffer information of RADIUS accounting-stop packets.

Format

reset radius-server accounting-stop-packet { **all** | **ip** { *ipv4-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Clears statistics on the remaining buffer information of RADIUS accounting-stop packets.	-
ip *ipv4-address*	Clears statistics on the remaining buffer information of RADIUS accounting-stop packets with the specified IPv4 address.	The value of *ipv4-address* is in dotted decimal notation.
ip *ipv6-address*	Clears statistics on the remaining buffer information of RADIUS accounting-stop packets with the specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command can clear statistics on the remaining buffer information of RADIUS accounting-stop packets. The deleted statistics cannot be restored.

Example

Clear statistics on the remaining buffer information of all RADIUS accounting-stop packets.


```
<HUAWEI> reset radius-server accounting-stop-packet all
```

13.2.68 test-aaa

Function

The **test-aaa** command tests the connectivity between the device and the authentication server or accounting server, and tests whether a user can be authenticated using authentication server and whether the accounting server can charge a user.

Format

test-aaa *user-name user-password* **radius-template** *template-name* [**chap** | **pap**] [**called-station-id** [**ssid** *ssid*]]

test-aaa *user-name user-password* **radius-template** *template-name* [**accounting** [**start** | **realtime** | **stop**]]

test-aaa *user-name user-password* **hwtacacs-template** *template-name* [**accounting** [**start** | **realtime** | **stop**]]

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **ssid** parameter.

Parameters

Parameter	Description	Value
user-name	Specifies a user name.	The value is a string of 1 to 253 case-insensitive characters. When the user name contains spaces, you must put the string in double quotation marks (""). **NOTE** When the HWTACACS, or RADIUS server is detected, the user name cannot contain spaces.

Parameter	Description	Value
user-password	Specifies a user password.	The value is a string of 1 to 128 case-sensitive characters.
radius-template *template-name*	Specifies the name of a RADIUS server template.	The RADIUS server template must already exist.
chap	Indicates Challenge Handshake Authentication Protocol (CHAP) authentication. The NAS device sends the user name, password, and 16-byte random code to the RADIUS server. The RADIUS server searches for the database according to the user name and obtains the password that is the same as the encrypted password at the user side. The RADIUS server then encrypts the received 16-byte random code and compares the result with the password. If they are the same, the user is authenticated. If they are different, the user fails to be authenticated. In addition, if the user is authenticated, the RADIUS server generates a 16-byte random code to challenge the user.	-
pap	Indicates Password Authentication Protocol (PAP) authentication. The NAS device adds the user name and encrypted password to the corresponding fields of authentication request packets, and then sends the packets to the RADIUS server. The NAS device determines whether to allow the user go online based on the result returned by the RADIUS server.	-

Parameter	Description	Value
called-station-id	Specifies the called-station-id attribute. When the device detects that an authentication packet carries the called-station-id attribute, it automatically encapsulates its MAC address XX-XX-XX-XX-XX-XX. The MAC address format is configured in the RADIUS server template.	-

Parameter	Description	Value
ssid *ssid*	Specifies the SSID.	The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or the combination of Chinese and English characters, without tab characters. To start an SSID with a space, you need to enclose the SSID with double quotation marks ("), for example, **" hello"**. The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to put a backslash (\) before the double quotation mark, for example, **\"hello**. The backslash occupies one character.
accounting	Indicates accounting. By default, an accounting-start packet is sent.	-

Parameter	Description	Value
start	Indicates that the sent packet is an accounting-start packet.	-
realtime	Indicates that the sent packet is a real-time accounting packet.	-
stop	Indicates that the sent packet is an accounting-stop packet.	-
hwtacacs-template *template-name*	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The test-aaa command tests service reachability of the server. The device sends an authentication or accounting request packet to the server. If the server returns an authentication or accounting success packet, the device and server can communicate with each other. If the server's response times out, the device and server cannot communicate with each other.

When the controller functions as an authentication server and the **test-aaa** command is run to test accounts, authentication packets must carry the user name, password, device MAC address, and SSID (for wireless terminals) so that the controller can match the packets with the corresponding authentication template. This ensures that the function of the **test-aaa** command is working properly.

Prerequisites

The authentication server template or accounting server template has been created, and the authentication server or accounting server has been configured in the template. In addition, the authentication server or accounting server has been configured.

Follow-up Procedure

If the test result indicates that the user fails to be authenticated by using server authentication or the accounting server fails to charge the user, check whether the configuration of the authentication server template and the authentication server is correct, and check the connectivity between the device and the server.

Precautions

chap and **pap** are two authentication modes, CHAP authentication is used by default.

- PAP: The NAS device adds the user name and encrypted password to the corresponding fields of authentication request packets, and then sends the packets to the RADIUS server. The NAS device determines whether to allow the user go online based on the result returned by the RADIUS server.
- CHAP: The NAS device sends the user name, password, and 16-byte random code to the RADIUS server. The RADIUS server searches for the database according to the user name and obtains the password that is the same as the encrypted password at the user side. The RADIUS server then encrypts the received 16-byte random code and compares the result with the password. If they are the same, the user is authenticated. If they are different, the user fails to be authenticated. In addition, if the user is authenticated, the RADIUS server generates a 16-byte random code to challenge the user.

Before running the **test-aaa** command, you only need to create a RADIUS server template and specify an authentication server or accounting server in the RADIUS server template.

Example

Test whether the user **user1** can be authenticated using CHAP authentication in the RADIUS server template **test**.

```
<HUAWEI> test-aaa user1 userkey radius-template test chap
Info: The server template does not exist.
```

13.3 HWTACACS Configuration Commands

13.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.3.2 display hwtacacs-server accounting-stop-packet

Function

The **display hwtacacs-server accounting-stop-packet** command displays information about Accounting-Stop packets sent by an HWTACACS server.

Format

display hwtacacs-server accounting-stop-packet { **all** | *number* | **ip** { *ipv4-address* | *ipv6-address* }}

Parameters

Parameter	Description	Value
all	Displays information about all Accounting-Stop packets.	-
number	Specifies the number of pieces of Accounting-Stop information that can be queried by each process.	The value is an integer that ranges from 1 to 65535.
ip *ipv4-address*	Displays information about Accounting-Stop packets sent by the HWTACACS server with a specified IPv4 address.	The value is in dotted decimal notation.
ip *ipv6-address*	Displays information about Accounting-Stop packets sent by the HWTACACS server with a specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

All views

Default Level

3: Management level

Usage Guidelines

During HWTACACS troubleshooting, you can run this command to check information about Accounting-Stop packets sent by the HWTACACS server.

NOTE

After an active/standby switchover, statistics about Accounting-Stop packets will be cleared.

Example

Display information about all Accounting-Stop packets.

```
<HUAWEI> display hwtacacs-server accounting-stop-packet all
------------------------------------------------------------
NO. SendTime      IP Address                Template
1   10            192.168.1.110             tac
------------------------------------------------------------
Whole accounting stop packet to resend:1
```


Table 13-35 Description of the **display hwtacacs-server accounting-stop-packet** command output

Item	Description
NO.	Number of the Accounting-Stop packet.
SendTime	Number of times that Accounting-Stop packets are sent.
IP Address	IP address of the HWTACACS server.
Template	Name of the HWTACACS server template.
Whole accounting stop packet to resend	Total number of Accounting-Stop packets sent by a device.

13.3.3 display hwtacacs-server template

Function

The **display hwtacacs-server template** command displays the configurations of HWTACACS server templates.

Format

display hwtacacs-server template [*template-name*]

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display hwtacacs-server template** command output helps you check the configurations of HWTACACS server templates and locate faults.

NOTE

The device determines whether its communication with the HWTACACS server is proper based on the response timeout mechanism of HWTACACS request packets, and always marks the status of the last HWTACACS server as Up.

Example

Display the configuration of the HWTACACS server template **template0**.

```
<HUAWEI> display hwtacacs-server template template0
  ------------------------------------------------------------------------------
  HWTACACS-server template name        : template0
  HWTACACS-server template index       : 0
  Primary-authentication-server        : -:49 Vrf:- Status:-

  Primary-authentication-ipv6-server   : -:49 Vrf:- Status:-
  Primary-authorization-server         : -:49 Vrf:- Status:-
  Primary-authorization-ipv6-server    : -:49 Vrf:- Status:-
  Primary-accounting-server            : -:49 Vrf:- Status:-
  Primary-accounting-ipv6-server       : -:49 Vrf:- Status:-
  Secondary-authentication-server      : -:49 Vrf:- Status:-
  Secondary-authentication-ipv6-server : -:49 Vrf:- Status:-
  Secondary-authorization-server       : -:49 Vrf:- Status:-
  Secondary-authorization-ipv6-server  : -:49 Vrf:- Status:-
  Secondary-accounting-server          : -:49 Vrf:- Status:-
  Secondary-accounting-ipv6-server     : -:49 Vrf:- Status:-
  Third-authentication-server          : -:49 Vrf:- Status:-
  Third-authentication-ipv6-server     : -:49 Vrf:- Status:-
  Third-authorization-server           : -:49 Vrf:- Status:-
  Third-authorization-ipv6-server      : -:49 Vrf:- Status:-
  Third-accounting-server              : -:49 Vrf:- Status:-
  Third-accounting-ipv6-server         : -:49 Vrf:- Status:-
  Fourth-authentication-server         : -:49 Vrf:- Status:-
  Fourth-authentication-ipv6-server    : -:49 Vrf:- Status:-
  Fourth-authorization-server          : -:49 Vrf:- Status:-
  Fourth-authorization-ipv6-server     : -:49 Vrf:- Status:-
  Fourth-accounting-server             : -:49 Vrf:- Status:-
  Fourth-accounting-ipv6-server        : -:49 Vrf:- Status:-
  Current-authentication-server        : -:49 Vrf:- Status:-
  Current-authentication-ipv6-server   : -:49 Vrf:- Status:-
  Current-authorization-server         : -:49 Vrf:- Status:-
  Current-authorization-ipv6-server    : -:49 Vrf:- Status:-
  Current-accounting-server            : -:49 Vrf:- Status:-
  Current-accounting-ipv6-server       : -:49 Vrf:- Status:-
  Source-IP-address                    : -
  Source-LoopBack                      : -
  Source-Vlanif                        : -
  Source-IPv6-address                  : -
  IPv6 Source-LoopBack                 : -
  IPv6 Source-Vlanif                   : -
  Shared-key                           : -
  Quiet-interval(min)                  : 5
  Response-timeout-Interval(sec)       : 5
  Domain-included                      : Original
  Traffic-unit                         : B
  User name in authen-start message    : Yes
  ------------------------------------------------------------------------------
```

Table 13-36 Description of the **display hwtacacs-server template** command output

Item	Description
HWTACACS-server template name	Name of an HWTACACS server template.
HWTACACS-server template index	Index of an HWTACACS server template.
Primary-authentication-server	IPv4 address, port number, VPN instance, and status of the primary authentication server.
Primary-authentication-ipv6-server	IPv6 address, port number, VPN instance, and status of the primary authentication server.
Primary-authorization-server	IPv4 address, port number, VPN instance, and status of the primary authorization server.
Primary-authorization-ipv6-server	IPv6 address, port number, VPN instance, and status of the primary authorization server.
Primary-accounting-server	IPv4 address, port number, VPN instance, and status of the primary accounting server.
Primary-accounting-ipv6-server	IPv6 address, port number, VPN instance, and status of the primary accounting server.
Secondary-authentication-server	IPv4 address, port number, VPN instance, and status of the second authentication server.
Secondary-authentication-ipv6-server	IPv6 address, port number, VPN instance, and status of the second authentication server.
Secondary-authorization-server	IPv4 address, port number, VPN instance, and status of the second authorization server.
Secondary-authorization-ipv6-server	IPv6 address, port number, VPN instance, and status of the second authorization server.
Secondary-accounting-server	IPv4 address, port number, VPN instance, and status of the second accounting server.
Secondary-accounting-ipv6-server	IPv6 address, port number, VPN instance, and status of the second accounting server.
Third-authentication-server	IPv4 address, port number, VPN instance, and status of the third authentication server.
Third-authentication-ipv6-server	IPv6 address, port number, VPN instance, and status of the third authentication server.
Third-authorization-server	IPv4 address, port number, VPN instance, and status of the third authorization server.

Item	Description
Third-authorization-ipv6-server	IPv6 address, port number, VPN instance, and status of the third authorization server.
Third-accounting-server	IPv4 address, port number, VPN instance, and status of the third accounting server.
Third-accounting-ipv6-server	IPv6 address, port number, VPN instance, and status of the third accounting server.
Fourth-authentication-server	IPv4 address, port number, VPN instance, shared key, and status of the fourth authentication server.
Fourth-authentication-ipv6-server	IPv6 address, port number, VPN instance, shared key, and status of the fourth authentication server.
Fourth-authorization-server	IPv4 address, port number, VPN instance, shared key, and status of the fourth authorization server.
Fourth-authorization-ipv6-server	IPv6 address, port number, VPN instance, shared key, and status of the fourth authorization server.
Fourth-accounting-server	IPv4 address, port number, VPN instance, shared key, and status of the fourth accounting server.
Fourth-accounting-ipv6-server	IPv6 address, port number, VPN instance, shared key, and status of the fourth accounting server.
Current-authentication-server	IPv4 address, port number, VPN instance, and status of the authentication server in use.
Current-authentication-ipv6-server	IPv6 address, port number, VPN instance, and status of the authentication server in use.
Current-authorization-server	IPv4 address, port number, VPN instance, and status of the authorization server in use.
Current-authorization-ipv6-server	IPv6 address, port number, VPN instance, and status of the authorization server in use.
Current-accounting-server	IPv4 address, port number, VPN instance, and status of the accounting server in use.
Current-accounting-ipv6-server	IPv6 address, port number, VPN instance, and status of the accounting server in use.
Source-IP-address	Source IPv4 address for communication between the device and the HWTACACS server.
Source-LoopBack	Number of the loopback interface. The IPv4 address of the loopback interface is used as the source IPv4 address for communication between the device and the HWTACACS server.

Item	Description
Source-Vlanif	Number of the VLANIF interface. The IPv4 address of the VLANIF interface is used as the source IPv4 address for communication between the device and the HWTACACS server.
Source-IPv6-address	Source IPv6 address for communication between the device and the HWTACACS server.
IPv6 Source-LoopBack	Number of the loopback interface. The IPv6 address of the loopback interface is used as the source IPv6 address for communication between the device and the HWTACACS server.
IPv6 Source-Vlanif	Number of the VLANIF interface. The IPv6 address of the VLANIF interface is used as the source IPv6 address for communication between the device and the HWTACACS server.
Shared-key	Shared key of the HWTACACS server.
Quiet-interval(min)	Interval for the primary server to return to the active state, in minutes.
Response-timeout-Interval(sec)	Response timeout interval of the HWTACACS server, in seconds.
Domain-included	Whether the user name contains an authentication domain name. ● Yes: The user name contains the domain name. ● No: The user name does not contain the domain name. ● Original: The device does not modify the user name entered by the user.
Traffic-unit	Traffic unit used by the HWTACACS server, in bytes.
User name in authen-start message	Whether the Authentication-Start packet of an administrator carries a user name: ● Yes: The Authentication-Start packet of an administrator carries a user name. ● No: The Authentication-Start packet of an administrator does not carry a user name.

13.3.4 display hwtacacs-server template verbose

Function

The **display hwtacacs-server template verbose** command displays statistics on HWTACACS authentication, accounting, and authorization.

Format

display hwtacacs-server template *template-name* **verbose**

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

By viewing statistics on HWTACACS authentication, accounting, and authorization, administrators can better understand the interaction between modules, facilitating fault locating and troubleshooting.

You can run the **reset hwtacacs-server statistics** { **all** | **accounting** | **authentication** | **authorization** } command to delete statistics on HWTACACS authentication, accounting, and authorization.

Precautions

In the HWTACACS server template, you can query the relevant statistics only after the IP address of the authentication server, the IP address of the authorization server, or the IP address of the accounting server is configured.

Example

Display statistics on HWTACACS authentication, accounting, and authorization in the HWTACACS server template *test1*.

```
<HUAWEI> display hwtacacs-server template test1 verbose
---[HWTACACS template test1 primary
authentication]---
HWTACACS server open number:
1670281960
HWTACACS server close number: 508333868
HWTACACS authen client access request packet number:
0
HWTACACS authen client access response packet number:
0
HWTACACS authen client unknown type number:
0
HWTACACS authen client timeout number: 0
```



```
HWTACACS authen client packet dropped number:
0
HWTACACS authen client access request change password number:
0
HWTACACS authen client access request login number:
0
HWTACACS authen client access request send authentication number:
0
HWTACACS authen client access request send password number:
0
HWTACACS authen client access connect abort number:
0
HWTACACS authen client access connect packet number:
0
HWTACACS authen client access response error number:
0
HWTACACS authen client access response failure number:
0
HWTACACS authen client access response follow number:
0
HWTACACS authen client access response getdata number:
0
HWTACACS authen client access response getpassword number:
0
HWTACACS authen client access response getuser number:
0
HWTACACS authen client access response pass number:
0
HWTACACS authen client access response restart number:
0
HWTACACS authen client malformed access response number:
0
HWTACACS authen client round trip time(s): 0
---[HWTACACS template test1 primary
authorization]---
HWTACACS server open number:
1670281960
HWTACACS server close number: 508333868
HWTACACS author client request packet number:
0
HWTACACS author client response packet number:
0
HWTACACS author client timeout number: 0
HWTACACS author client packet dropped number:
0
HWTACACS author client unknown type number:
0
HWTACACS author client request EXEC number:
0
HWTACACS author client request PPP number: 0
HWTACACS author client request VPDN number:
0
HWTACACS author client response error number:
0
HWTACACS author client response EXEC number:
0
HWTACACS author client response PPP number:
0
HWTACACS author client response VPDN number:
0
HWTACACS author client round trip time(s): 0
---[HWTACACS template test1 primary
accounting]---
HWTACACS server open number:
1670281960
HWTACACS server close number: 508333868
HWTACACS account client request packet number:
0
HWTACACS account client response packet number:
```



```
0
HWTACACS account client unknown type number:
0
HWTACACS account client timeout number: 0
HWTACACS account client packet dropped number:
0
HWTACACS account client request command level number:
0
HWTACACS account client request connection number:
0
HWTACACS account client request EXEC number:
0
HWTACACS account client request network number:
0
HWTACACS account client request system event number:
0
HWTACACS account client request update number:
0
HWTACACS account client response error number:
0
HWTACACS account client round trip time(s): 0
```


Table 13-37 Description of the **display hwtacacs-server template verbose** command output

Item	Description
HWTACACS template test1 primary authentication	Statistics on the primary authentication server in the HWTACACS server template *test1*. If the secondary and third authentication servers are configured, the relevant statistics are also displayed, including: • HWTACACS server open number: Number of times that the socket connection of the HWTACACS server is set up • HWTACACS server close number: Number of times that the socket connection of the HWTACACS server is disconnected • HWTACACS authen client access request packet number: Number of HWTACACS client authentication request packets • HWTACACS authen client access response packet number: Number of HWTACACS client authentication response packets • HWTACACS authen client unknown type number: Number of unknown HWTACACS client authentication messages • HWTACACS authen client timeout number: Number of HWTACACS client authentication timeouts • HWTACACS authen client packet dropped number: Number of times that HWTACACS client authentication packets are dropped • HWTACACS authen client access request change password number: Number of password change requests from an HWTACACS client • HWTACACS authen client access request login number: Number of HWTACACS client login requests • HWTACACS authen client access request send authentication number: Number of authentication requests sent by an HWTACACS client • HWTACACS authen client access request send password number: Number of times that an HWTACACS client sends passwords • HWTACACS authen client access connect abort number: Number of connection-stop packets sent by an HWTACACS client • HWTACACS authen client access connect packet number: Number of continuous packets sent by an HWTACACS client • HWTACACS authen client access response error number: Number of error packets received by an HWTACACS client

Item	Description
	• HWTACACS authen client access response failure number: Number of authentication failure packets received by an HWTACACS client • HWTACACS authen client access response follow number: Number of packets that an HWTACACS client receives from the server for re-authentication • HWTACACS authen client access response getdata number: Number of packets that an HWTACACS client receives from the server for user information • HWTACACS authen client access response getpassword number: Number of packets that an HWTACACS client receives from the server for user password • HWTACACS authen client access response getuser number: Number of packets that an HWTACACS client receives from the server for user name • HWTACACS authen client access response pass number: Number of authentication success packets received by an HWTACACS client • HWTACACS authen client access response restart number: Number of authentication restart packets that an HWTACACS client receives from the server • HWTACACS authen client malformed access response number: Number of invalid response packets received by an HWTACACS client • HWTACACS authen client round trip time(s): Last authentication response time of the HWTACACS server

Item	Description
HWTACACS template test1 primary authorization	Statistics on the primary authorization server in the HWTACACS server template *test1*. If the secondary and third authorization servers are configured, the relevant statistics are also displayed, including: • HWTACACS server open number: Number of times that the socket connection of the HWTACACS server is set up • HWTACACS server close number: Number of times that the socket connection of the HWTACACS server is disconnected • HWTACACS author client request packet number: Number of HWTACACS client authorization request packets • HWTACACS author client response packet number: Number of HWTACACS client authorization response packets • HWTACACS author client timeout number: Number of HWTACACS client authorization timeouts • HWTACACS author client packet dropped number: Number of times that HWTACACS client authorization packets are dropped • HWTACACS author client unknown type number: Number of unknown authorization packets on an HWTACACS client • HWTACACS author client request EXEC number: Number of EXEC user request packets authorized by an HWTACACS client • HWTACACS author client request PPP number: Number of PPP user request packets authorized by an HWTACACS client • HWTACACS author client request VPDN number: Number of VPDN user request packets authorized by an HWTACACS client • HWTACACS author client response error number: Number of error authorization response packets received by an HWTACACS client • HWTACACS author client response EXEC number: Number of authorized EXEC user response packets received by an HWTACACS client • HWTACACS author client response PPP number: Number of authorized PPP user response packets received by an HWTACACS client • HWTACACS author client response VPDN number: Number of authorized VPDN user response packets received by an HWTACACS client • HWTACACS author client round trip time(s): Last authorization response time of the HWTACACS server

Item	Description
HWTACACS template test1 primary accounting	Statistics on the primary accounting server in the HWTACACS server template *test1*. If the secondary and third accounting servers are configured, the relevant statistics are also displayed, including: • HWTACACS server open number: Number of times that the socket connection of the HWTACACS server is set up • HWTACACS server close number: Number of times that the socket connection of the HWTACACS server is disconnected • HWTACACS account client request packet number: Number of HWTACACS client accounting request packets • HWTACACS account client response packet number: Number of HWTACACS client accounting response packets • HWTACACS account client unknown type number: Number of unknown HWTACACS client accounting packets • HWTACACS account client timeout number: Number of HWTACACS client accounting timeouts • HWTACACS account client packet dropped number: Number of times that HWTACACS client accounting packets are dropped • HWTACACS account client request command level number: Number of HWTACACS client accounting requests for command line packets • HWTACACS account client request connection number: Number of HWTACACS client accounting requests for connection • HWTACACS account client request EXEC number: Number of HWTACACS client accounting requests for EXEC packets • HWTACACS account client request network number: Number of HWTACACS client accounting requests for Network packets • HWTACACS account client request system event number: Number of HWTACACS client accounting requests for system event packets • HWTACACS account client request update number: Number of HWTACACS client accounting requests for update packets • HWTACACS account client response error number: Number of HWTACACS client accounting requests for error packets

Item	Description
	• HWTACACS account client round trip time(s): Response time of the last accounting packet of the HWTACACS server

13.3.5 hwtacacs enable

Function

The **hwtacacs enable** command enables Huawei Terminal Access Controller Access Control System (HWTACACS).

The **undo hwtacacs enable** command disables HWTACACS.

By default, HWTACACS is enabled.

Format

hwtacacs enable

undo hwtacacs enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To use HWTACACS authentication, authorization, or accounting, run the **hwtacacs enable** command to enable the HWTACACS function.

Precautions

If the **undo hwtacacs enable** command is run when a user is performing HWTACACS authentication, authorization, or accounting, the command does not take effect.

Example

Disable HWTACACS.


```
<HUAWEI> system-view
[HUAWEI] undo hwtacacs enable
```

13.3.6 hwtacacs-server

Function

The **hwtacacs-server** command applies an HWTACACS server template to a domain.

The **undo hwtacacs-server** command deletes an HWTACACS server template from a domain.

By default, no HWTACACS server template is applied to a domain.

Format

hwtacacs-server *template-name*

undo hwtacacs-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform HWTACACS authentication, authorization, and accounting for users in a domain, configure an HWTACACS server template in the domain. After the HWTACACS server template is configured in the domain, the configuration in the HWTACACS server template takes effect.

Prerequisites

An HWTACACS server template has been created by using the **hwtacacs-server template** command.

Example

Apply the HWTACACS server template **tacacs1** to the domain **tacacs1**.


```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template tacacs1
[HUAWEI-hwtacacs-tacacs1] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain tacacs1
[HUAWEI-aaa-domain-tacacs1] hwtacacs-server tacacs1
```

13.3.7 hwtacacs-server accounting

Function

The **hwtacacs-server accounting** command configures an HWTACACS accounting server.

The **undo hwtacacs-server accounting** command cancels the configuration.

By default, no HWTACACS accounting server is configured.

Format

hwtacacs-server accounting { *ipv4-address* | *ipv6-address* } [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third** | **fourth**]

undo hwtacacs-server accounting [**secondary** | **third** | **fourth**] { **ip-address** | **ipv6-address** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS accounting server.	The value is in dotted decimal notation. It must be a valid unicast address.
ipv6-address	Specifies the IPv6 address of an HWTACACS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of an HWTACACS accounting server.	The value is an integer that ranges from 1 to 65535. The default value is 49.
public-net	Indicates that the HWTACACS accounting server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the HWTACACS accounting server is bound to.	The value must be an existing VPN instance name.

Parameter	Description	Value
secondary	Configures the second HWTACACS accounting server as the secondary server. If no secondary server is configured, the primary HWTACACS accounting server is specified.	-
third	Specifies the third HWTACACS accounting server as the secondary server. If no secondary server is configured, the primary HWTACACS accounting server is specified.	-
fourth	Specifies the fourth HWTACACS accounting server as the secondary server. If no secondary server is configured, the primary HWTACACS accounting server is specified.	-
ip-address	Deletes the primary HWTACACS accounting server with a specified IPv4 address. If the secondary server is specified, the secondary HWTACACS accounting server with the specified IPv4 address is deleted.	-
ipv6-address	Deletes the primary HWTACACS accounting server with a specified IPv6 address. If the secondary server is specified, the secondary HWTACACS accounting server with the specified IPv4 address is deleted.	-

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device does not support local accounting; therefore, you need to configure an HWTACACS accounting server to perform accounting. The device sends accounting packets to an HWTACACS accounting server only after the accounting server is specified in an HWTACACS server template.

Precautions

- You can modify this configuration only when device does not set up TCP connection with the specified accounting server.
- The IP addresses of the primary and secondary servers must be different. Otherwise, the server configuration fails.
- If the command is run for multiple times in the same HWTACACS server template to configure the servers with the same IP protocol stack and type (for example, the servers are all IPv4 primary servers), only the latest configuration takes effect.
- IPv4 and IPv6 servers are configured at the same time in the same HWTACACS server template. The order for selecting servers is as follows: primary IPv4 server -> primary IPv6 server -> second secondary IPv4 server -> second secondary IPv6 server -> third secondary IPv4 server -> third secondary IPv6 server -> fourth secondary IPv4 server -> fourth secondary IPv6 server.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

Example

Configure the primary HWTACACS accounting server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server accounting 10.163.155.12 52
```


13.3.8 hwtacacs-server accounting-stop-packet resend

Function

The **hwtacacs-server accounting-stop-packet resend** command enables or disables retransmission of accounting-stop packets and sets the number of accounting-stop packets that can be retransmitted each time.

By default, 100 accounting-stop packets can be retransmitted each time.

Format

hwtacacs-server accounting-stop-packet resend { **disable** | **enable** *number* }

Parameters

Parameter	Description	Value
disable	Disables the retransmission of accounting-stop packets.	-
enable *number*	Enables the retransmission of accounting-stop packets, and specifies the number of packets that can be retransmitted each time.	The value is an integer that ranges from 1 to 300.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a user goes offline, the device sends an accounting-stop packet to an accounting server. After the accounting server receives the accounting-stop packet, it stops accounting for the user. If the accounting server does not receive the accounting-stop packet because of network faults, it continues to perform accounting for the user. As a result, the user is charged incorrectly. To solve this problem, configure the device to send accounting-stop packets multiple times.

Precautions

- If **disable** is configured, an accounting-stop packet is transmitted only once even when packet transmission fails.

- If **enable** *number* is configured, *number* specifies the number of accounting-stop packets that can be retransmitted each time when the device does not receive any response packet from the HWTACACS server or fails to receive the response packet.

Example

Enable the retransmission of accounting-stop packets and set the number of accounting-stop packets that can be retransmitted each time to 50.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server accounting-stop-packet resend enable 50
```

13.3.9 hwtacacs-server authentication

Function

The **hwtacacs-server authentication** command configures the HWTACACS authentication server.

The **undo hwtacacs-server authentication** command deletes configurations of the HWTACACS authentication server.

By default, no HWTACACS authentication server is configured.

Format

hwtacacs-server authentication { *ipv4-address* | *ipv6-address* } [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third** | **fourth**]

undo hwtacacs-server authentication [**secondary** | **third** | **fourth**] { **ip-address** | **ipv6-address** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS authentication server.	The value is in dotted decimal notation. It must be a valid unicast address.
ipv6-address	Specifies the IPv6 address of an HWTACACS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of an HWTACACS authentication server.	The value is an integer that ranges from 1 to 65535. The default value is 49.

Parameter	Description	Value
public-net	Indicates that the HWTACACS authentication server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the HWTACACS authentication server is bound to.	The value must be an existing VPN instance name.
secondary	Configures the second HWTACACS authentication server as the secondary server. If no secondary server is configured, the primary HWTACACS authentication server is specified.	-
third	Configures the third HWTACACS authentication server as the secondary server. If no secondary server is configured, the primary HWTACACS authentication server is specified.	-
fourth	Specifies the fourth HWTACACS authentication server as the secondary server. If no secondary server is configured, the primary HWTACACS authentication server is specified.	-
ip-address	Deletes the primary HWTACACS authentication server with a specified IPv4 address. If the secondary server is specified, the secondary HWTACACS authentication server with the specified IPv4 address is deleted.	-

Parameter	Description	Value
ipv6-address	Deletes the primary HWTACACS authentication server with a specified IPv6 address. If the secondary server is specified, the secondary HWTACACS authentication server with the specified IPv6 address is deleted.	-

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users in HWTACACS mode, you must configure the HWTACACS authentication server. When both the primary and secondary authentication servers are configured, the device sends an authentication request packet to the secondary authentication server in any of the following situations:

- The device fails to send a request packet to the primary authentication server.
- If the device does not receive any authentication response packet from the primary server:
- The primary authentication server requires re-authentication.
- The primary authentication server considers that the received authentication request packet is incorrect.

Precautions

- You can modify this configuration only when device does not set up TCP connection with the specified accounting server.
- The IP addresses of the primary and secondary servers must be different. Otherwise, the server configuration fails.
- If the command is run for multiple times in the same HWTACACS server template to configure the servers with the same IP protocol stack and type (for example, the servers are all IPv4 primary servers), only the latest configuration takes effect.
- IPv4 and IPv6 servers are configured at the same time in the same HWTACACS server template. The order for selecting servers is as follows: primary IPv4 server -> primary IPv6 server -> second secondary IPv4 server -> second secondary IPv6 server -> third secondary IPv4 server -> third

secondary IPv6 server -> fourth secondary IPv4 server -> fourth secondary IPv6 server.

- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

Example

Configure the primary HWTACACS authentication server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server authentication 10.163.155.12 49
```

13.3.10 hwtacacs-server authentication user-name in-authentication-start

Function

The **hwtacacs-server authentication user-name in-authentication-start** command configures a user name to be carried in the Authentication Start packet of an administrator.

The **undo hwtacacs-server authentication user-name in-authentication-start** command configures a user name not to be carried in the Authentication Start packet of an administrator.

By default, the Authentication Start packet of an administrator does not carry a user name.

Format

hwtacacs-server authentication user-name in-authentication-start

undo hwtacacs-server authentication user-name in-authentication-start

Parameters

None

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the Authentication Start packet sent by the device to the HWTACACS server does not carry a user name. When the device connects to a specific server, the server identifies whether a user is an administrator based on the user name carried in the Authentication Start packet received from the device. To configure a user name to be carried in the Authentication Start packet of an administrator, run the **hwtacacs-server authentication user-name in-authentication-start** command.

Precautions

- This function takes effect only for administrators.
- This command does not take effect if it is independently executed. It takes effect only after the **undo hwtacacs-server user-name domain-included** command is executed.

Example

Configure a user name to be carried in the Authentication Start packet of an administrator.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server authentication user-name in-authentication-start
```

13.3.11 hwtacacs-server authorization

Function

The **hwtacacs-server authorization** command configures the HWTACACS authorization server.

The **undo hwtacacs-server authorization** command deletes configurations of the HWTACACS authorization server.

By default, no HWTACACS authorization server is configured.

Format

hwtacacs-server authorization { *ipv4-address* | *ipv6-address* } [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third** | **fourth**]

undo hwtacacs-server authorization [**secondary** | **third** | **fourth**] { **ip-address** | **ipv6-address** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS authorization server.	The value is in dotted decimal notation. It must be a valid unicast address.
ipv6-address	Specifies the IPv6 address of an HWTACACS authorization server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of an HWTACACS authorization server.	The value is an integer that ranges from 1 to 65535. The default value is 49.
public-net	Indicates that the HWTACACS authorization server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the HWTACACS authorization server is bound to.	The value must be an existing VPN instance name.
secondary	Configures the second HWTACACS authorization server as the secondary server. If no secondary server is configured, the primary HWTACACS authorization server is specified.	-
third	Configures the third HWTACACS authorization server as the secondary server. If no secondary server is configured, the primary HWTACACS authorization server is specified.	-

Parameter	Description	Value
fourth	Specifies the fourth HWTACACS authorization server as the secondary server. If no secondary server is configured, the primary HWTACACS authorization server is specified.	-
ip-address	Deletes the primary HWTACACS authorization server with a specified IPv4 address. If the secondary server is specified, the secondary HWTACACS authorization server with the specified IPv4 address is deleted.	-
ipv6-address	Deletes the primary HWTACACS authorization server with a specified IPv6 address. If the secondary server is specified, the secondary HWTACACS authorization server with the specified IPv6 address is deleted.	-

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authorize users in HWTACACS mode, you must configure the HWTACACS authorization server.

Precautions

- You can modify this configuration only when device does not set up TCP connection with the specified accounting server.

- The IP addresses of the primary and secondary servers must be different. Otherwise, the server configuration fails.
- If the command is run for multiple times in the same HWTACACS server template to configure the servers with the same IP protocol stack and type (for example, the servers are all IPv4 primary servers), only the latest configuration takes effect.
- IPv4 and IPv6 servers are configured at the same time in the same HWTACACS server template. The order for selecting servers is as follows: primary IPv4 server -> primary IPv6 server -> second secondary IPv4 server -> second secondary IPv6 server -> third secondary IPv4 server -> third secondary IPv6 server -> fourth secondary IPv4 server -> fourth secondary IPv6 server.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

Example

Configure the primary HWTACACS authorization server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server authorization 10.163.155.12 49
```

13.3.12 hwtacacs-server shared-key

Function

The **hwtacacs-server shared-key** command sets a shared key for an HWTACACS server.

The **undo hwtacacs-server shared-key** command cancels the configuration.

By default, the HWTACACS server is not configured with any shared key.

Format

hwtacacs-server shared-key cipher *key-string*

undo hwtacacs-server shared-key

Parameters

Parameter	Description	Value
cipher	Indicates the shared key in cipher text.	-
key-string	Specifies a shared key.	The value is a string of case-sensitive characters. It cannot contain question marks (?) and spaces. The key is processed as cipher text no matter whether the **cipher** keyword is specified. The *key-string* may be a plain text consisting of 1 to 255 characters or a cipher text consisting of 20 to 392 characters.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with an HWTACACS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. The device and HWTACACS server must use the same key to ensure their validity in the authentication.

Precautions

For security purposes, it is recommended that the password contains at least two types of lowercase letters, uppercase letters, numerals, and special characters, and contains at least 8 characters.

You can modify this configuration only when the HWTACACS server template is not in use.

During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

Example

Set the shared key of the HWTACACS server to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server shared-key cipher YsHsjx_202206
```


13.3.13 hwtacacs-server source-ip

Function

The **hwtacacs-server source-ip** command specifies the source IPv4 address used by a device to communicate with an HWTACACS server.

The **undo hwtacacs-server source-ip** command cancels the configuration.

By default, the device uses the IPv4 address of the actual outbound interface as the source IPv4 address encapsulated in HWTACACS packets.

Format

hwtacacs-server source-ip *ip-address*

hwtacacs-server source-ip source-loopback *interface-number*

hwtacacs-server source-ip source-vlanif *interface-number*

undo hwtacacs-server source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IPv4 address for communication between the device and HWTACACS server.	The value is a valid unicast address in dotted decimal notation.
source-loopback *interface-number*	Specifies the IPv4 address of the loopback interface as the source IPv4 address for communication between the device and HWTACACS server.	The loopback interface must already exist.
source-vlanif *interface-number*	Specifies the IPv4 address of the VLANIF interface as the source IPv4 address for communication between the device and HWTACACS server.	The VLANIF interface must already exist.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

You can configure all HWTACACS packets sent by the device to use the same source IPv4 address. In this way, an HWTACACS server uses only one IPv4 address to communicate with the device.

If an interface connecting the device to a server has multiple IP addresses configured and can communicate with the server only through some of these IP addresses, one IP address among these reachable IP addresses needs to be specified as the source IP address based on the routing table to ensure that the device can communicate with the server.

If you run this command multiple times, only the latest configuration takes effect.

Example

Specify the source IPv4 address 10.1.1.1 for communication between the device and HWTACACS server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server source-ip 10.1.1.1
```

13.3.14 hwtacacs-server source-ipv6

Function

The **hwtacacs-server source-ipv6** command specifies the source IPv6 address used by a device to communicate with an HWTACACS server.

The **undo hwtacacs-server source-ipv6** command cancels the configuration.

By default, the device uses the IPv6 address of the actual outbound interface as the source IPv6 address encapsulated in HWTACACS packets.

Format

hwtacacs-server source-ipv6 *ipv6-address*

hwtacacs-server source-ipv6 source-loopback *interface-number*

hwtacacs-server source-ipv6 source-vlanif *interface-number*

undo hwtacacs-server source-ipv6

Parameters

Parameter	Description	Value
ipv6-address	Specifies the source IPv6 address for communicating with the HWTACACS server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
source-loopback *interface-number*	Specifies the IPv6 address of the loopback interface as the source IPv6 address for communicating with the HWTACACS server.	The loopback interface must already exist.
source-vlanif *interface-number*	Specifies the IPv6 address of the VLANIF interface as the source IPv6 address for communicating with the HWTACACS server.	The VLANIF interface must already exist.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

After you specify the source IPv6 address in HWTACACS packets, the device uses this IPv6 address to communicate with the HWTACACS server.

If an interface connecting the device to a server has multiple IP addresses configured and can communicate with the server only through some of these IP addresses, one IP address among these reachable IP addresses needs to be specified as the source IP address based on the routing table to ensure that the device can communicate with the server.

If you run this command multiple times, only the latest configuration takes effect.

Example

Specify the source IPv6 address fc00::1 in HWTACACS packets.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server source-ipv6 fc00::1
```

13.3.15 hwtacacs-server template

Function

The **hwtacacs-server template** command creates an HWTACACS server template and enters the HWTACACS server template view.

The **undo hwtacacs-server template** command deletes an HWTACACS server template.

By default, no HWTACACS server template is configured.

Format

hwtacacs-server template *template-name*

undo hwtacacs-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The value is a string of 1 to 32 case-sensitive characters. The name contains only letters, digits (0-9), dots (.), underscores (_) and hyphens (-), and a combination of the above characters. The value cannot be - or --.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can perform HWTACACS configurations, such as the configuration of authentication servers, authorization servers, accounting servers, and shared key, only after an HWTACACS server template is created.

Follow-up Procedure

Configure an authentication server, accounting server, and shared key in the HWTACACS server template view, and run the **hwtacacs-server** command in the domain view to apply the HWTACACS server template.

Precautions

You can delete a template only when the template is not in use.

Example

Create an HWTACACS server template **template1** and enter the HWTACACS server template view.


```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template template1
[HUAWEI-hwtacacs-template1]
```

13.3.16 hwtacacs-server timer quiet

Function

The **hwtacacs-server timer quiet** command sets the quiet interval before the primary server reverts to the active state.

The **undo hwtacacs-server timer quiet** command restores the default quiet interval before the primary server reverts to the active state.

By default, the quiet interval before the primary HWTACACS server reverts to the active state is 5 minutes.

Format

hwtacacs-server timer quiet *interval*

undo hwtacacs-server timer quiet

Parameters

Parameter	Description	Value
interval	Specifies the quiet interval before the primary server reverts to the active state.	The value is an integer ranging from 0 to 255, in minutes.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the primary server is unavailable, the device automatically switches services to the standby server and sends packets to the standby server. After the quiet interval before the primary server reverts to the active state expires, the device attempts to establish a connection with the primary server.

- If the primary server is still unavailable, the device continues to send packets to the standby server until the next interval expires. Such a process repeats.
- If the primary server is available, the device switches services to the primary server and sends packets to the primary server.

The quiet interval before the primary server reverts to the active state ensures that the primary server can be restored immediately and reduces the number of detection times during the switchover.

The default value is recommended.

Precautions

When the quiet interval of the active server is set to 0, if the active server fails, the device sends packets to the standby server. When the active server is recovered, the device does not connect to the active server, but still sends packets to the standby server until the standby server fails.

When you run the **hwtacacs-server timer quiet** command to change the quiet interval before the primary server reverts to the active state, the device does not check whether the HWTACACS server template is in use.

Example

Set the quiet interval before the primary server reverts to the active state to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template template1
[HUAWEI-hwtacacs-template1] hwtacacs-server timer quiet 3
```

13.3.17 hwtacacs-server timer response-timeout

Function

The **hwtacacs-server timer response-timeout** command sets the response timeout interval of an HWTACACS server.

The **undo hwtacacs-server timer response-timeout** command restores the default response timeout interval of an HWTACACS server.

By default, the response timeout interval for an HWTACACS server is 5 seconds.

Format

hwtacacs-server timer response-timeout *interval*

undo hwtacacs-server timer response-timeout

Parameters

Parameter	Description	Value
interval	Specifies the response timeout interval of an HWTACACS server.	The value is an integer ranging from 1 to 300, in seconds.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the device sends a request packet to the HWTACACS server, if the device does not receive any response packet from the server within the specified response timeout interval:

- If only one HWTACACS server is configured, the device does not retransmit the request to this server.
- If both active/standby HWTACACS servers are available and the TCP link between them works normally, the device retransmits the request to the standby server after timeout. If the TCP link is broken during the timeout interval, the device immediately retransmits the request to the standby server.

This improves reliability of HWTACACS authentication, authorization, and accounting.

The default value is recommended.

Precautions

You can modify this configuration only when the HWTACACS server template is not in use.

Example

Set the response timeout interval of an HWTACACS server to 30s.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server timer response-timeout 30
```

13.3.18 hwtacacs-server traffic-unit

Function

The **hwtacacs-server traffic-unit** command sets the traffic unit used by an HWTACACS server.

The **undo hwtacacs-server traffic-unit** command restores the default traffic unit used by the HWTACACS server.

By default, the traffic unit is byte on the device.

Format

hwtacacs-server traffic-unit { **byte** | **kbyte** | **mbyte** | **gbyte** }

undo hwtacacs-server traffic-unit

Parameters

Parameter	Description	Value
byte	Indicates that the traffic unit is byte.	-
kbyte	Indicates that the traffic unit is KByte.	-
mbyte	Indicates that the traffic unit is MByte.	-
gbyte	Indicates that the traffic unit is GByte.	-

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Different HWTACACS servers may use different traffic units; therefore, you need to set the traffic unit for each HWTACACS server group on the device and the traffic unit must be the same as that on the HWTACACS server.

Precautions

You can modify this configuration only when the HWTACACS server template is not in use.

Example

Set the traffic unit used by an HWTACACS server to KByte.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template template1
[HUAWEI-hwtacacs-template1] hwtacacs-server traffic-unit kbyte
```

13.3.19 hwtacacs-server user-name domain-included

Function

The **hwtacacs-server user-name domain-included** command configures the device to encapsulate the domain name in the user name in HWTACACS packets to be sent to an HWTACACS server.

The **hwtacacs-server user-name original** command configures the device not to modify the user name entered by the user in the packets sent to the HWTACACS server.

The **undo hwtacacs-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name when sending HWTACACS packets to an HWTACACS server.

By default, the device encapsulates the domain name in the user name when sending HWTACACS packets to an HWTACACS server.

By default, the device does not modify the user name entered by the user in the packets sent to the HWTACACS server.

Format

hwtacacs-server user-name domain-included

hwtacacs-server user-name original

undo hwtacacs-server user-name domain-included

Parameters

None

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The format of a user name is user name@domain name. In the user name, @ is the domain name delimiter.

If the HWTACACS server does not accept the user name with the domain name, run the **undo hwtacacs-server user-name domain-included** command to delete the domain name from the user name.

Precautions

You can modify this configuration only when the HWTACACS server template is not in use.

If the user names in the HWTACACS packets sent from the device to HWTACACS server contain domain names, ensure that the total length of a user name (user name + domain name delimiter + domain name) is not longer than 64 characters; otherwise, the user name cannot be contained in HWTACACS packets. As a result, authentication will fail.

Example

Configure the device to encapsulate the domain name in the user name when sending HWTACACS packets to an HWTACACS server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template template1
[HUAWEI-hwtacacs-template1] hwtacacs-server user-name domain-included
```

13.3.20 hwtacacs-user change-password hwtacacs-server

Function

The **hwtacacs-user change-password hwtacacs-server** command enables the device to change the passwords saved on the HWTACACS server.

Format

hwtacacs-user change-password hwtacacs-server *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

To change the password saved on the HWTACACS server, users can run the **hwtacacs-user change-password hwtacacs-server** command on the device. You do not need to change the configuration on the HWTACACS server.

Precautions

- Users are HWTACACS authenticated and the HWTACACS server template is configured.
- Users can run this command to change the passwords only when the user names and passwords saved on the HWTACACS do not expire. When a user whose password has expired logs in to the device, the HWTACACS server does not allow the user to change the password and displays a message indicating that the authentication fails.

- The system wait period is 30 seconds. If the TACACS server does not receive the user name, new password, or confirmed password from the user within such a period, it terminates the password change process.
- Users can also press **Ctrl+C** to cancel password change.
- HWTACACS users who pass AAA authentication can use the **hwtacacs-user change-password hwtacacs-server** command to change the passwords before the passwords expire. If a user needs to run this command to change the passwords of other users, the user must have the administrative rights.

Example

Enable the user that passes HWTACACS authentication to change the password.

```
<HUAWEI> hwtacacs-user change-password hwtacacs-server example
Username:cj@example
Old Password:
New Password:
Re-enter New password:
Info: The password has been changed successfully.
```

13.3.21 reset hwtacacs-server accounting-stop-packet

Function

The **reset hwtacacs-server accounting-stop-packet** command clears statistics on Accounting Stop packets.

Format

reset hwtacacs-server accounting-stop-packet { **all** | **ip** { *ipv4-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Clears the statistics about all accounting-stop packets.	-
ip *ipv4-address*	Clears the statistics about the Accounting-Stop packets sent by the HWTACACS server with a specified IPv4 address.	The value is in dotted decimal notation.
ip *ipv6-address*	Clears the statistics about the Accounting-Stop packets sent by the HWTACACS server with a specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

Statistics cannot be restored once being cleared.

Example

Clear statistics on all Accounting Stop packets.

```
<HUAWEI> reset hwtacacs-server accounting-stop-packet all
```

13.3.22 reset hwtacacs-server statistics

Function

The **reset hwtacacs-server statistics** command clears the statistics on HWTACACS authentication, accounting, and authorization.

Format

reset hwtacacs-server statistics { **all** | **accounting** | **authentication** | **authorization** }

Parameters

Parameter	Description	Value
all	Clears all the statistics.	-
accounting	Clears the statistics on HWTACACS accounting.	-
authentication	Clears the statistics on HWTACACS authentication.	-
authorization	Clears the statistics on HWTACACS authorization.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If statistics about HWTACACS authentication, accounting, and authorization need to be collected in a specified period of time, you must clear the original statistics first.

Precautions

- After the **reset hwtacacs-server statistics** command is run, all the statistics about HWTACACS authentication, accounting, and authorization is cleared. In addition, the statistics cannot be restored once being cleared. Therefore, exercise caution when you decide to run this command.
- You can run the **display hwtacacs-server template** *template-name* **verbose** command to check statistics about HWTACACS authentication, accounting, and authorization in the specified server template.

Example

Clear all the statistics.

```
<HUAWEI> reset hwtacacs-server statistics all
```

13.4 HACA Configuration Commands

13.4.1 Command Support

Only the following switch models support HACA:

S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H and S6720S-S

13.4.2 display haca-server accounting-stop-packet all

Function

The **display haca-server accounting-stop-packet all** command displays information about all accounting-stop packets on the HACA server.

Format

display haca-server accounting-stop-packet all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display haca-server accounting-stop-packet all** command output helps you check configurations or locate HACA server faults.

Example

View information about all accounting-stop packets on the HACA server.

```
<HUAWEI> display haca-server accounting-stop-packet all
--------------------------------------------------------------------------------
 Time Stamp  Resend Times  Session Time
Username
 --------------------------------------------------------------------------------
3245884970  32           49           123
 --------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 13-38 Description of the **display haca-server accounting-stop-packet all** command output

Item	Description
Time Stamp	Timestamp of an accounting-stop packet.
Resend Times	Number of times that accounting-stop packets have been retransmitted.
Session Time	Session time, in seconds.
Username	User name.

13.4.3 display haca-server configuration

Function

The **display haca-server configuration** command displays the HACA server template configuration.

Format

display haca-server configuration [**template** *template-name*]

Parameters

Parameter	Description	Value
template *template-name*	Specifies the name of an HACA server template. If this parameter is not specified, the configurations of all HACA server templates are displayed.	The HACA server template name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an HACA server template is configured or during HACA troubleshooting, you can run this command to check whether the HACA server template is correctly configured.

Example

Display the HACA server template configuration.

```
<HUAWEI> display haca-server configuration
  ------------------------------------------------------------------------------
  HACA-server template name : default
  HACA-server server-address dynamic : Enable
  HACA-server server-ip-address(port) : 1.2.3.4(50300)
  HACA-server pki-realm-name : default
  HACA-server status : IDLE
  HACA-server escape-state : UP
  HACA-server down-delay-interval in use(sec) : -
  HACA-server heart-beat-interval in use(min) : -
  HACA-server reconnection-interval in use(min) : -
  HACA-server register-sync-interval in use(min) : -
  HACA-bak-server server-ip-address(port) : -(0)
  HACA-bak-server pki-realm-name : -
  HACA-bak-server status : -
  HACA-bak-server escape-state : -
  HACA-bak-server down-delay-interval in use(sec) : -
  HACA-bak-server heart-beat-interval in use(min) : -
  HACA-bak-server reconnection-interval in use(min) : -
  HACA-bak-server register-sync-interval in use(min) : -
  Configured source-ip-address : -
  Configured down-delay-interval(sec) : 30
  Configured response-timeout-interval(sec) : 5
  Configured domain-included : ORIGINAL
  Configured heart-beat-interval(min) : 5
  Configured reconnection-interval(min) : 1
  Configured user-syn-interval(min) : 10
  Configured register-sync-interval(min) : 15
```



```
Configured accounting-stop-packet resend : 3
------------------------------------------------------------------------------
```

Table 13-39 Description of the **display haca-server configuration** command output

Item	Description
HACA-server template name	Name of an HACA server template. To configure this parameter, run the **haca-server template** command.
HACA-server server-address dynamic	Whether the HACA server dynamic address function to support dynamic IP address switching is enabled. ● Enable ● Disable
HACA-server server-ip-address(port)	IP address and port number of the HACA server. To configure this parameter, run the **haca-server server-address** command.
HACA-server pki-realm-name	PKI realm name of the HACA server. To configure this parameter, run the **haca-server server-address** command.
HACA-server Status	Status of the HACA server: ● IDLE: idle state ● INIT: initial state ● UP: Up state ● REGISTER: registration state ● DOWN: Down state
HACA-server escape-state	HACA server escape state: ● UP: The escape path will not be used. ● ESCAPE: The escape path is being prepared. ● -: The server is in initial state, and the escape path will not be used.
HACA-server down-delay-interval in use(sec)	Delay after which the HACA server in use is disconnected, in seconds. To configure this parameter, run the **haca-server timer down-delay** command.

Item	Description
HACA-server heart-beat-interval in use(min)	Interval at which heartbeat packets of the HACA server in use are sent, in minutes. To configure this parameter, run the **haca-server timer heart-beat** command.
HACA-server reconnection-interval in use(min)	Interval at which the HACA server in use is reconnected, in minutes. To configure this parameter, run the **haca-server timer reconnection**.
HACA-server register-sync-interval in use(min)	Interval at which registration synchronization packets of the HACA server in use are sent, in minutes. To configure this parameter, run the **haca-server timer register-sync** command.
HACA-bak-server server-ip-address(port)	IP address and port number of the secondary HACA server. To configure this parameter, run the **haca-server server-address** command.
HACA-bak-server pki-realm-name	PKI realm name of the secondary HACA server. To configure this parameter, run the **haca-server server-address** command.
HACA-bak-server Status	Status of the secondary HACA server: ● IDLE: idle state ● INIT: initial state ● UP: Up state ● REGISTER: registration state ● DOWN: Down state
HACA-bak-server escape-state	Escape state of the secondary HACA server: ● UP: The escape path will not be used. ● ESCAPE: The escape path is being prepared. ● -: The server is in initial state, and the escape path will not be used.

Item	Description
HACA-bak-server down-delay-interval in use(sec)	Delay after which the secondary HACA server in use is disconnected, in seconds. To configure this parameter, run the **haca-server timer down-delay** command.
HACA-bak-server heart-beat-interval in use(min)	Interval at which heartbeat packets of the secondary HACA server in use are sent, in minutes. To configure this parameter, run the **haca-server timer heart-beat** command.
HACA-bak-server reconnection-interval in use(min)	Interval at which the secondary HACA server in use is reconnected, in minutes. To configure this parameter, run the **haca-server timer reconnection**.
HACA-bak-server register-sync-interval in use(min)	Interval at which registration synchronization packets of the secondary HACA server are sent, in minutes. To configure this parameter, run the **haca-server timer register-sync** command.
Configured source-ip-address	Source IP address of HACA packets. To configure this parameter, run the **haca-server source-ip** command.
Configured down-delay-interval(sec) :	Delay after which an HACA server is disconnected, in seconds. To configure this parameter, run the **haca-server timer down-delay** command.
Configured response-timeout-interval(sec)	HACA packet response timeout period, in seconds. To configure this parameter, run the **haca-server timer response-timeout** command.

Item	Description
Configured domain-included	HACA user name format (whether a user name contains a domain name): • YES: The user name contains a domain name. • NO: The user name does not contain a domain name. • ORIGINAL: The device does not modify the user name entered by the user. To configure this parameter, run the **haca-server user-name** command.
Configured heart-beat-interval(min)	Interval at which HACA heartbeat packets are sent, in minutes. To configure this parameter, run the **haca-server timer heart-beat** command.
Configured reconnection-interval(min)	Interval at which an HACA server is reconnected, in minutes. To configure this parameter, run the **haca-server timer reconnection** command.
Configured user-syn-interval(min)	Interval at which HACA user information is synchronized, in minutes. To configure this parameter, run the **haca-server timer user-syn** command.
Configured register-sync-interval(min)	Interval at which registration synchronization packets are sent, in minutes. To configure this parameter, run the **haca-server timer register-sync** command.
Configured accounting-stop-packet resend	Number of times that HACA Accounting-Stop packets are retransmitted. To set this parameter, run the **haca-server accounting-stop-packet resend** command.

13.4.4 display haca-server statistics

Function

The **display haca-server statistics** command displays HACA packet statistics.

Format

display haca-server statistics { **all** | **message** | **packet** [**authentication** | **authorization** | **accounting** | **cut-notify** | **cut-request** | **register** | **user-syn**] } [**template** *template-name*]

Parameters

Parameter	Description	Value
all	Displays statistics about all packets.	-
message	Displays statistics about messages.	-
packet	Displays statistics about the specified type of packets.	-
authentication	Displays statistics about authentication packets.	-
authorization	Displays statistics about authorization packets.	-
accounting	Displays statistics about accounting packet.	-
cut-notify	Displays statistics about logout notification packets.	-
cut-request	Displays statistics about logout request packets.	-
register	Displays statistics about registration packets.	-
user-syn	Displays statistics about user synchronization packets.	-
template *template-name*	Displays packet statistics about the specified HACA server template.	The HACA server template must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

During fault location, you can run this command to view statistics about HACA packets.

Example

Display HACA packet statistics.

```
<HUAWEI> display haca-server statistics all
------------------------------------------------------------------
Haca-server Template haca Statistics:
------------------------------------------------------------------
Authen_Request_Messages                          = 0
Authen_Accept_Messages                           = 0
Authen_Reject_Messages                           = 0
Author_Request_Messages                          = 0
Author_Accept_Messages                           = 0
Author_Reject_Messages                           = 0
Coa_Request_Messages                             = 0
Coa_Accept_Messages                              = 0
Coa_Reject_Messages                              = 0
Account_Start_Messages                           = 0
Account_RT_Messages                              = 0
Account_Stop_Messages                            = 0
Account_StartAck_Messages                        = 0
Account_RTAck_Messages                           = 0
Account_StopAck_Messages                         = 0
Account_StartAckFail_Messages                    = 0
Account_RTAckFail_Messages                       = 0
Account_StopAckFail_Messages                     = 0
UserSyn_Request_To_Server_Messages               = 0
UserSyn_Response_From_Server_Messages            = 0
UserSyn_Request_From_Server_Messages             = 0
UserSyn_Response_To_Server_Messages              = 0
Cut_Request_Messages                             = 0
Cut_Response_Messages                            = 0
Cut_Notify_Messages                              = 0
Send_to_HacaServer_RegRequest_Packets            = 0
Received_from_HacaServer_RegResponse_Packets     = 0
Error_Send_to_HacaServer_RegRequest_Packets      = 0
Error_Received_from_HacaServer_RegResponse_Packets = 0
Send_to_HacaServer_AuthenRequest_Packets         = 0
Received_from_HacaServer_AuthenAccept_Packets    = 0
Received_from_HacaServer_AuthenReject_Packets    = 0
Error_Send_to_HacaServer_AuthenRequest_Packets   = 0
Error_Received_from_HacaServer_AuthenAccept_Packets = 0
Error_Received_from_HacaServer_AuthenReject_Packets = 0
Received_from_HacaServer_AuthorRequest_Packets   = 0
Send_to_HacaServer_AuthorAccept_Packets          = 0
Send_to_HacaServer_AuthorReject_Packets          = 0
Error_Received_from_HacaServer_AuthorRequest_Packets = 0
Error_Send_to_HacaServer_AuthorAccept_Packets    = 0
Error_Send_to_HacaServer_AuthorReject_Packets    = 0
Received_from_HacaServer_CoaRequest_Packets      = 0
Send_to_HacaServer_CoaAccept_Packets             = 0
Send_to_HacaServer_CoaReject_Packets             = 0
Error_Received_from_HacaServer_CoaRequest_Packets = 0
Error_Send_to_HacaServer_CoaAccept_Packets       = 0
Error_Send_to_HacaServer_CoaReject_Packets       = 0
Received_from_HacaServer_AcctSucc_Packets        = 0
Send_to_HacaServer_AcctSend_Packets              = 0
Error_Received_from_HacaServer_AcctFail_Packets  = 0
```



```
Error_Send_to_HacaServer_AcctSendFail_Packets          = 0
Send_to_HacaServer_UserSynRequest_Packets              = 0
Received_from_HacaServer_UserSynResponse_Packets       = 0
Send_to_HacaServer_UserSynRespons_Packets              = 0
Received_from_HacaServer_UserSynRequest_Packets        = 0
Error_Send_to_HacaServer_UserSynRequest_Packets        = 0
Error_Received_from_HacaServer_UserSynResponse_Packets = 0
Error_Send_to_HacaServer_UserSynRespons_Packets        = 0
Error_Received_from_HacaServer_UserSynRequest_Packets  = 0
Send_to_HacaServer_CutNotify_Packets                   = 0
Error_Send_to_HacaServer_CutNotify_Packets             = 0
Received_from_HacaServer_CutRequest_Packets            = 0
Send_to_HacaServer_CutResponse_Packets                 = 0
Error_Received_from_HacaServer_CutRequest_Packets      = 0
Error_Send_to_HacaServer_CutResponse_Packets           = 0
------------------------------------------------------------------
```

Table 13-40 Description of the **display haca-server statistics** command output

Item	Description
Haca-server Template haca Statistics	Statistics about the HACA server template haca.
Authen_Request_Messages	Statistics about authentication request messages.
Authen_Accept_Messages	Statistics about access-accept messages.
Authen_Reject_Messages	Statistics about access-reject messages.
Author_Request_Messages	Statistics about authorization request messages.
Author_Accept_Messages	Statistics about authorization-accept messages.
Author_Reject_Messages	Statistics about authorization-reject messages.
Coa_Request_Messages	Statistics about CoA request messages.
Coa_Accept_Messages	Statistics about CoA-accept messages.
Coa_Reject_Messages	Statistics about CoA-reject messages.
Account_Start_Messages	Statistics about accounting-start request messages.
Account_RT_Messages	Statistics about real-time accounting request messages.
Account_Stop_Messages	Statistics about accounting-stop request messages.
Account_StartAck_Messages	Statistics about accounting-start response success messages.

Item	Description
Account_RTAck_Messages	Statistics about real-time accounting response success messages.
Account_StopAck_Messages	Statistics about accounting-stop response success messages.
Account_StartAckFail_Messages	Statistics about accounting-start response failure messages.
Account_RTAckFail_Messages	Statistics about real-time accounting response failure messages.
Account_StopAckFail_Messages	Statistics about accounting-stop response failure messages.
UserSyn_Request_To_Server_Messages	Statistics about user synchronization request messages sent to the HACA server.
UserSyn_Response_From_Server_Messages	Statistics about user synchronization response messages received from the HACA server.
UserSyn_Request_From_Server_Messages	Statistics about user synchronization request messages received from the HACA server.
UserSyn_Response_To_Server_Messages	Statistics about user synchronization response messages sent to the HACA server.
Cut_Request_Messages	Statistics about logout request messages.
Cut_Response_Messages	Statistics about logout response messages.
Cut_Notify_Messages	Statistics about logout notification messages.
Send_to_HacaServer_RegRequest_Packets	Statistics about registration request messages sent to the HACA server.
Received_from_HacaServer_RegResponse_Packets	Statistics about registration response messages received from the HACA server.
Error_Send_to_HacaServer_RegRequest_Packets	Statistics about error registration request messages sent to the HACA server.
Error_Received_from_HacaServer_RegResponse_Packets	Statistics about error registration response messages received from the HACA server.
Send_to_HacaServer_AuthenRequest_Packets	Statistics about authentication request messages sent to the HACA server.
Received_from_HacaServer_AuthenAccept_Packets	Statistics about authentication response messages received from the HACA server.

Item	Description
Received_from_HacaServer_AuthenReject_Packets	Statistics about access-reject messages received from the HACA server.
Error_Send_to_HacaServer_AuthenRequest_Packets	Statistics about error authentication request messages sent to the HACA server.
Error_Received_from_HacaServer_AuthenAccept_Packets	Statistics about error authentication response messages received from the HACA server.
Error_Received_from_HacaServer_AuthenReject_Packets	Statistics about error access-reject messages received from the HACA server.
Received_from_HacaServer_AuthorRequest_Packets	Statistics about authorization request messages received from the HACA server.
Send_to_HacaServer_AuthorAccept_Packets	Statistics about authorization response messages sent to the HACA server.
Send_to_HacaServer_AuthorReject_Packets	Statistics about authorization-reject messages sent to the HACA server.
Error_Received_from_HacaServer_AuthorRequest_Packets	Statistics about error authorization request messages received from the HACA server.
Error_Send_to_HacaServer_AuthorAccept_Packets	Statistics about error authorization response messages sent to the HACA server.
Error_Send_to_HacaServer_AuthorReject_Packets	Statistics about error authorization-reject messages sent to the HACA server.
Received_from_HacaServer_CoaRequest_Packets	Statistics about CoA request messages received from the HACA server.
Send_to_HacaServer_CoaAccept_Packets	Statistics about CoA response messages sent to the HACA server.
Send_to_HacaServer_CoaReject_Packets	Statistics about CoA-reject messages sent to the HACA server.
Error_Received_from_HacaServer_CoaRequest_Packets	Statistics about error CoA request messages received from the HACA server.
Error_Send_to_HacaServer_CoaAccept_Packets	Statistics about error CoA response messages sent to the HACA server.

Item	Description
Error_Send_to_HacaServer_CoaReject_Packets	Statistics about error CoA-reject messages sent to the HACA server.
Received_from_HacaServer_AcctSucc_Packets	Statistics about the received accounting response success messages.
Send_to_HacaServer_AcctSend_Packets	Statistics about the sent accounting request success messages.
Error_Received_from_HacaServer_AcctFail_Packets	Statistics about the received accounting request failure messages.
Error_Send_to_HacaServer_AcctSendFail_Packets	Statistics about the sent accounting request failure messages.
Send_to_HacaServer_UserSynRequest_Packets	Statistics about user synchronization request messages sent to the HACA server.
Received_from_HacaServer_UserSynResponse_Packets	Statistics about user synchronization response messages received from the HACA server.
Send_to_HacaServer_UserSynRespons_Packets	Statistics about user synchronization response messages sent to the HACA server.
Received_from_HacaServer_UserSynRequest_Packets	Statistics about user synchronization request messages received from the HACA server.
Error_Send_to_HacaServer_UserSynRequest_Packets	Statistics about error user synchronization request messages sent to the HACA server.
Error_Received_from_HacaServer_UserSynResponse_Packets	Statistics about error user synchronization response messages received from the HACA server.
Error_Send_to_HacaServer_UserSynRespons_Packets	Statistics about error user synchronization response messages sent to the HACA server.
Error_Received_from_HacaServer_UserSynRequest_Packets	Statistics about error user synchronization request messages received from the HACA server.
Send_to_HacaServer_CutNotify_Packets	Statistics about user logout notification messages sent to the HACA server.

Item	Description
Error_Send_to_HacaServer_CutNotify_Packets	Statistics about error user logout notification messages sent to the HACA server.
Received_from_HacaServer_CutRequest_Packets	Statistics about error user logout request messages received from the HACA server.
Send_to_HacaServer_CutResponse_Packets	Statistics about user logout request messages sent to the HACA server.
Error_Received_from_HacaServer_CutRequest_Packets	Statistics about error user logout request messages received from the HACA server.
Error_Send_to_HacaServer_CutResponse_Packets	Statistics about error user logout response messages sent to the HACA server.

13.4.5 haca enable

Function

The **haca enable** command enables the HACA function.

The **undo haca enable** command disables the HACA function.

By default, HACA is disabled.

Format

haca enable

undo haca enable

Parameters

None

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The authentication server is located on the cloud, so packets between the device and server must traverse the NAT device. However, Portal protocol packets cannot traverse the NAT device. HACA implements communication between the device and server, and then Portal authentication can be performed.

If you require HACA authentication, run the **haca enable** command to enable HACA.

Prerequisites

The IP address and port number of the HACA server have been configured using the **haca-server server-address** command.

Example

Enable HACA.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server server-address 10.1.1.1 default
[HUAWEI-haca-haca] haca enable
```

13.4.6 haca-server (AAA domain view)

Function

The **haca-server** command applies an HACA server template to a domain.

The **undo haca-server** command unbinds an HACA server template from a domain.

By default, no HACA server template is configured in a domain.

Format

haca-server *template-name*

undo haca-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HACA server template.	The HACA server template must exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform HACA authentication for users in a domain, apply an HACA server template to the domain. An HACA server template takes effect only after the HACA server template is applied to the domain.

Precautions

An HACA server template has been created by using the **haca-server template** command.

Example

Apply the HACA server template **haca** to the domain **test**.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] haca-server haca
```

13.4.7 haca-server accounting-stop-packet resend

Function

The **haca-server accounting-stop-packet resend** command enables retransmission of accounting-stop packets and sets the number of accounting-stop packets that can be retransmitted.

The **undo haca-server accounting-stop-packet resend** command disables retransmission of accounting-stop packets.

By default, three accounting-stop packets can be retransmitted.

Format

haca-server accounting-stop-packet resend [*resend-times*]

undo haca-server accounting-stop-packet resend

Parameters

Parameter	Description	Value
resend-times	Specifies the number of retransmitted accounting-stop packets.	The value is an integer that ranges from 0 to 300.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Accounting-stop packets cannot be forwarded to an HACA server that is unreachable. You can run the **haca-server accounting-stop-packet resend** command to save the accounting-stop packets in the buffer and send them at the preset intervals until the number of allowed retransmission times is reached or the packets are sent successfully.

Example

Enable the retransmission of accounting-stop packets and set the number of accounting-stop packets that can be retransmitted to 50.

```
<HUAWEI> system-view
[HUAWEI] haca-server template test1
[HUAWEI-haca-test1] haca-server accounting-stop-packet resend 50
```

13.4.8 haca-server server-address

Function

The **haca-server server-address** command configures the IP address and port number for the HACA server.

The **undo haca-server server-address** command deletes the IP address and port number configured for the HACA server.

By default, the IP address and port number of the HACA server are not configured on the device.

Format

haca-server server-address *ip-address* [*port*] *pki-realm-name* [**backup**]

undo haca-server server-address [*ip-address* [*port*]] [**backup**]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an HACA server.	The value is in dotted decimal notation. It must be a valid unicast address.

Parameter	Description	Value
port	Specifies the port number of an HACA server. If the parameter is not specified, the default value is used.	The value is an integer that ranges from 1 to 65535. The default value is 50300.
pki-realm-name	Specifies the name of a PKI domain.	The value must be an existing PKI domain name. **NOTE** If the specified PKI domain is the default domain, there may be security risks.
backup	Specifies the secondary HACA server.	-

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device needs to be connected to an HACA server for authentication. The HACA server is located on the Internet. Therefore, the device sends authentication packets to the HACA server only after the IP address and port number of the HACA server are specified.

Precautions

When you run the **haca enable** command, the system checks whether there is the primary HACA server. The standby HACA server takes effect only when the primary HACA server is configured.

Example

Configure the IP address of the HACA server to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server server-address 10.1.1.1 abc
```


13.4.9 haca-server server-address dynamic

Function

The **haca-server server-address dynamic** command enables the HACA server dynamic address function to support dynamic IP address switching.

The **undo haca-server server-address dynamic** command disables the HACA server dynamic address function.

By default, the HACA server dynamic address function is disabled.

Format

haca-server server-address dynamic [*port*] *pki-realm-name*

undo haca-server server-address [**dynamic** [*port*]]

Parameters

Parameter	Description	Value
port	Specifies the port number of an HACA server. If this parameter is not specified, the default value is used.	The value is an integer that ranges from 1 to 65535. The default port number is 50300.
pki-realm-name	Specifies the name of a PKI realm.	The value must be an existing PKI realm name. **NOTE** If the specified PKI realm is the default realm, there may be security risks.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the iMaster NCE-Campus active/standby scenario, devices establish connections with the HACA server. When the active device is not operational, the HACA server IP address on the device must support dynamic switching so that the standby device can take on the active role and re-establish a connection with the HACA

server. In this case, run this command to enable the HACA server dynamic address function to support dynamic IP address switching.

Precautions

In the VRRP hot standby scenario, a PKI realm needs to be created on the backup device to be bound to the HACA server.

The **haca-server server-address** *ip-address* [*port*] *pki-realm-name* [**backup**] and **haca-server server-address dynamic** [*port*] *pki-realm-name* commands are mutually exclusive and cannot be both configured.

Example

Enable the HACA server dynamic address function to support dynamic IP address switching.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server server-address dynamic 50301 default
```

13.4.10 haca-server source-ip

Function

The **haca-server source-ip** command configures a source IP address for the device to communicate with an HACA server.

The **undo haca-server source-ip** restores the default setting.

By default, no source IP address is configured for HACA packets. The device uses the IP address of the actual outbound interface as the source IP address of HACA packets.

Format

haca-server source-ip *ip-address*

undo haca-server source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for communication with an HACA server.	The value is in dotted decimal notation. It must be a valid unicast address.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

To communicate with an HACA server, the device sends packets encapsulated with source IP addresses. By default, the device uses the IP addresses of the actual outbound interfaces as the source IP address. This leads to a waste of IP addresses, and complicates the configuration. To simplify the configuration, run the **haca-server source-ip** command to set a same source IP address for all HACA packets. In this way, the HACA server can use only one IP address to communicate with the device.

Example

Set the source IP address for communication between the device and an HACA server to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server source-ip 10.1.1.1
```

13.4.11 haca-server template

Function

The **haca-server template** command creates an HACA server template and displays the HACA server template view.

The **undo haca-server template** command deletes an HACA server template.

By default, no HACA server template is created.

Format

haca-server template *template-name*

undo haca-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HACA server template.	The value is a string of 1 to 32 case-sensitive characters. The name contains only letters, digits (0-9), dots (.), underscores (_) and hyphens (-). It cannot be - or --.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure HACA authentication, you must create an HACA server template. You can perform HACA configurations, such as setting the IP address and interval of HACA heartbeat packets, only after an HACA server template is created.

Follow-up Procedure

After creating an HACA template, set the HACA server IP address and interval of the HACA heartbeat packets in the HACA server template view, and perform other configurations. Then, run the **haca-server** in the domain view to apply the HACA server template.

Example

Create an HACA server template **haca** and display the HACA server template view.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca]
```

13.4.12 haca-server timer down-delay

Function

The **haca-server timer down-delay** command sets the delay after which an HACA server is disconnected.

The **undo haca-server timer down-delay** command restores the default delay in which an HACA server is disconnected.

By default, the delay after which an HACA server is disconnected is 30s.

Format

haca-server timer down-delay *interval*

undo haca-server timer down-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay after which an HACA server is disconnected.	The value is an integer that ranges from 0 to 600, in seconds. Value 0 indicates that no delay is set for HACA server disconnection.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

If the communication between an HACA server and an access device is interrupted, authenticated users enter best-effort paths. That is, the users are allowed to access the network and will be reauthenticated after the communication re-establishes. If the HACA server is disconnected and connected frequently in a short period, a large number of users will be reauthenticated, which consumes device resources.

Therefore, set the delay after which an HACA server is disconnected to enable best-effort paths during the interval. When communication between the access devices and server is interrupted, the previously authenticated users will not be reauthenticated until the delay ends. This setting prevents resource exhaustion caused by frequent disconnection and reconnection.

Example

Set the delay after which an HACA server is disconnected to 60s.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer down-delay 60
```

13.4.13 haca-server timer heart-beat

Function

The **haca-server timer heart-beat** command sets the interval for sending HACA heartbeat packets.

The **undo haca-server timer heart-beat** command restores the default value of the interval for sending HACA heartbeat packets.

By default, the interval for sending HACA heartbeat packets is 5 minutes.

Format

haca-server timer heart-beat *interval*

undo haca-server timer heart-beat

Parameters

Parameter	Description	Value
interval	Specifies the interval at which HACA heartbeat packets are sent.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

A firewall may exist between the access device and HACA server. If the firewall does not detect packets for a long time, it may interrupt the connection. Run the **haca-server timer heart-beat** command to set the interval at which the client sends HACA heartbeat packets to ensure a proper connection.

Example

Set the interval for sending HACA heartbeat packets to 6 minutes.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer heart-beat 6
```

13.4.14 haca-server timer reconnection

Function

The **haca-server timer reconnection** command sets the reconnection interval for an HACA server.

The **undo haca-server timer reconnection** command restores the default value of the reconnection interval for an HACA server.

By default, the interval for reconnecting to an HACA server is one minute.

Format

haca-server timer reconnection *interval*

undo haca-server timer reconnection

Parameters

Parameter	Description	Value
interval	Specifies the interval for reconnecting to an HACA server.	The value is an integer that ranges from 1 to 255, in minutes.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

If the communication between an access device and an HACA server is interrupted, the device reconnects to the server immediately. If that reconnection fails, the device reconnects to HACA at the HACA reconnection interval until the connection succeeds.

Example

Set the reconnection interval for the HACA server to 2 minutes.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer reconnection 2
```

13.4.15 haca-server timer register-sync

Function

The **haca-server timer register-sync** command configures the interval for a device to send HACA registration synchronization packets to iMaster NCE-Campus.

The **undo haca-server timer register-sync** command restores the default settings.

By default, a device sends HACA registration synchronization packets to iMaster NCE-Campus at an interval of 15 minutes.

Format

haca-server timer register-sync *interval*

undo haca-server timer register-sync

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a device sends HACA registration synchronization packets to iMaster NCE-Campus.	The value is an integer in the range from 0 to 60, in minutes.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

You can run this command on a device so that the device sends HACA registration synchronization packets to iMaster NCE-Campus at the specified interval.

Example

Set the interval for a device to send HACA registration synchronization packets to iMaster NCE-Campus to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer register-sync 10
```

13.4.16 haca-server timer response-timeout

Function

The **haca-server timer response-timeout** command sets the response timeout interval for an HACA server.

The **undo haca-server timer response-timeout** command restores the default value of the response timeout interval for an HACA server.

By default, the response timeout interval for an HACA server is 5 seconds.

Format

haca-server timer response-timeout *interval*

undo haca-server timer response-timeout

Parameters

Parameter	Description	Value
interval	Specifies the response timeout interval of an HACA server.	It is an integer that ranges from 1 to 300, in seconds.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

A device may not receive the response packets from HACA after sending request packets to the server. After a response timeout interval is set, if a device does not receive response packets from the HACA server in that specified time after sending request packets, the device will send request packets again. This improves the reliability of HACA authentication.

Example

Set the response timeout interval for an HACA server to 30s.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer response-timeout 30
```

13.4.17 haca-server timer user-syn

Function

The **haca-server timer user-syn** command sets the interval for synchronizing user information for an HACA server.

The **undo haca-server timer user-syn** command restores the default value of the interval for synchronizing user information for an HACA server.

By default, the user information synchronization interval for an HACA server is 10 minutes.

Format

haca-server timer user-syn *interval*

undo haca-server timer user-syn

Parameters

Parameter	Description	Value
interval	Specifies the user information synchronization interval for an HACA server.	The value can be 0 or range from 3 to 65535, in minutes. The value **0** indicates that user information synchronization is disabled.

Views

System view

Default Level

3: Management level

Usage Guidelines

In HACA authentication application, if communication between the device and HACA server is interrupted due to a network failure or HACA server failure, online HACA users cannot go offline normally. As a result, user information on the device may be different from that on the HACA server, causing inaccurate accounting. Run the **haca-server timer user-syn** *interval* command to enable user information synchronization. Then user information will be synchronized between the device and HACA server at the interval, which ensures user information consistency.

Example

Set the user information synchronization interval for the HACA server to 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] haca-server timer user-syn 30
```

13.4.18 haca-server user-name

Function

The **haca-server user-name domain-included** command configures the device to encapsulate the domain name in the user name in HACA packets sent to an HACA server.

The **haca-server user-name original** command configures the device not to modify the user name entered by the user in the packets sent to the HACA server.

The **undo haca-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name when sending HACA packets to an HACA server.

By default, the device does not modify the user name entered by the user in the packets sent to the HACA server.

Format

haca-server user-name domain-included

haca-server user-name original

undo haca-server user-name domain-included

Parameters

None

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device manages access users based on domains. Each access user belongs to a domain. The users are authenticated in the specified domain when the entered user names contain domain names, or in the default domain when entered user names do not contain domain names. If a user name contains a domain name, the user belongs to that domain; otherwise, the user belongs to the default domain. When access users are authenticated in different domains, run the **haca-server user-name domain-included** command to configure the domain name encapsulated by the device in the user name in HACA packets to be sent to an HACA server.

The format of a user name is user name@domain name. In the user name, @ is the domain name delimiter. The domain name delimiter can also be any of the following symbols: \ / : < > | ' %.

If the HACA server does not accept the user name with the domain name, run the **undo haca-server user-name domain-included** command to delete the domain name from the user name.

Precautions

During Portal authentication, the **haca-server user-name domain-included** command does not take effect. During MAC address-prioritized Portal authentication, the **haca-server user-name domain-included** command takes effect only when users reconnect to the network through MAC address authentication.

Example

Configure the device not to encapsulate the domain name in the user name when sending HACA packets to an HACA server.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server user-name domain-included
```

13.4.19 reset haca-server statistics

Function

The **reset haca-server statistics** command clears HACA packet statistics.

Format

reset haca-server statistics { **all** | **message** | **packet** [**register** | **accounting** | **authentication** | **authorization** | **user-syn** | **cut-notify** | **cut-request**] }
[**template** *template-name*]

Parameters

Parameter	Description	Value
all	Clears all the statistics.	-
message	Clears all HACA message debugging information.	-
packet	Clears information about the specified type of packets.	-
register	Clears information about the registration packets.	-
accounting	Clears all statistics about HACA accounting.	-
authentication	Clears all statistics about HACA authentication.	-
authorization	Clears all statistics about HACA authorization.	-
user-syn	Clears all HACA user synchronization information.	-
cut-notify	Clears all HACA logout notifications.	-
cut-request	Clears all HACA logout requests.	-

Parameter	Description	Value
template *template-name*	Clears statistics about the specified HACA server template.	The HACA server template must already exist.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During fault location, you may need to collect statistics about the HACA packets in a certain period. Before collecting new statistics, clear the existing statistics. Then run the **display haca-server statistics** command to view HACA statistics.

Precautions

The **reset haca-server statistics** command clears statistics about HACA packets, and the cleared statistics cannot be restored. Therefore, exercise caution when running this command.

Example

Clear all HACA statistics.

```
<HUAWEI> reset haca-server statistics all
```

13.4.20 reset haca-server accounting-stop-packet all

Function

The **reset haca-server accounting-stop-packet all** command clears the remaining buffer information of all HACA accounting-stop packets.

Format

reset haca-server accounting-stop-packet all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run the **reset haca-server accounting-stop-packet all** command to clear the remaining buffer information of all HACA accounting-stop packets. Exercise caution when running this command because the information cannot be restored after being cleared.

Example

Clear the remaining buffer information of HACA accounting-stop packets.

```
<HUAWEI> reset haca-server accounting-stop-packet all
```

13.5 NAC Configuration Commands (Unified Mode)

13.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.5.2 access-context profile enable

Function

The **access-context profile enable** command enables the user context identification function.

The **undo access-context profile enable** command disables the user context identification function.

By default, the user context identification function is disabled.

Format

access-context profile enable

undo access-context profile enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User context refers to association information of a user, such as the user name, user VLAN, and access interface.

To simplify the authentication server configuration, the administrator can add the users with the same network access rights to the same user context profile based on the user context, and configure the network access rights for the users based on the user context profile. When a user goes online after the user context identification function is enabled, the device can identify the user context information and add the user to the corresponding context profile based on the identification result.

- If the user is authenticated successfully, the authentication server can assign the network access rights mapping the user context profile to the user based on the user context reported by the device.
- If the user fails to be authenticated, the device assigns the user the network access rights in each phase before authentication success, which are bound to the context profile in the user authentication event authorization policy.

For example, on some enterprise networks, VLANs are used to divide the entire network into different areas with various security levels. The administrator requires that a user should obtain different network access rights when the user connects to the network from different areas. In this case, the user context identification function can be enabled on access devices, and a group of VLANs that belong to the same area are added to the same user context profile. The administrator then assigns the mapping network access rights to different user context profiles based on the security level of each area. When a user connects to the network from different areas, the user is added to different user context profiles matching their access VLANs and therefore obtains different network access rights.

Follow-up Procedure

1. In the system view, run the **access-context profile name** *profile-name* command to create a user context profile.
2. In the user context profile view, run the **if-match vlan-id** { *start-vlan-id* [**to** *end-vlan-id*] } &<1-10> command to configure the user identification policy based on VLAN IDs.

Precautions

- The device can only identify user VLANs.

Example

Enable the user context identification function.

```
<HUAWEI> system-view
[HUAWEI] access-context profile enable
```


13.5.3 access-context profile name

Function

The **access-context profile name** command creates a user context profile and displays the user context profile view.

The **undo access-context profile name** command deletes the created user context profile.

By default, no user context profile is created.

Format

access-context profile name *profile-name*

undo access-context profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a user context profile.	The value is a string of 1 to 32 case-sensitive characters without any space. The value cannot be set to - or --, and cannot contain the following characters: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To simplify the authentication server configuration, the administrator can add the users with the same network access rights to the same user context profile based on the user context, and assign the network access rights to the users based on the user context profile.

Follow-up Procedure

In the user context profile view, run the **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] &<1-10> command to configure the user identification policy based on VLAN IDs.

Example

Creates the user context profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] access-context profile name p1
```

13.5.4 access-author policy global

Function

The **access-author policy global** command applies a user authentication event authorization policy.

The **undo access-author policy global** command restores the default configuration.

By default, no user authentication event authorization policy is applied.

Format

access-author policy *policy-name* **global**

undo access-author policy *policy-name* **global**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user authentication event authorization policy.	The value must be the name of an existing user authentication event authorization policy on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users need basic network access rights before they are authenticated. For example, the users need to download 802.1X clients and update the antivirus database. A user authentication event authorization policy can be used to bind the network access rights of users in each phase before authentication success to a user context profile. When a user goes online after a user authentication event authorization policy is applied to the device, the device adds the user to the

context profile based on the user context identification result, and assigns the network access rights to the user based on the user authentication result.

Prerequisites

A user authentication event authorization policy has been created using the **access-author policy name** *policy-name* command in the system view.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Only one user authentication event authorization policy can be applied globally. If you run this command multiple times, only the latest configuration takes effect.

Example

Globally apply the user authentication event authorization policy **a1**.

```
<HUAWEI> system-view
[HUAWEI] access-author policy name a1
[HUAWEI-access-author-a1] quit
[HUAWEI] access-author policy a1 global
```

13.5.5 access-author policy name

Function

The **access-author policy name** command creates a user authentication event authorization policy and displays the user authentication event authorization policy view.

The **undo access-author policy name** command deletes the created user authentication event authorization policy.

By default, no user authentication event authorization policy is created.

Format

access-author policy name *policy-name*

undo access-author policy name *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user authentication event authorization policy.	The value is a string of 1 to 32 case-sensitive characters without any space. The value cannot be set to - or --, and cannot contain the following characters: / \ : * ? " < > | @ ' %. **NOTE** The value of *profile-name* cannot be set to the first character or first several characters of the name, and the name itself, and it also cannot be the uppercase and lowercase combination of the first character, first several characters, and the name. This prevents the conflict with the **access-author policy global** command.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users need basic network access rights before they are authenticated. For example, the users need to download 802.1X clients and update the antivirus database. A user authentication event authorization policy can be used to bind the network access rights of users in each phase before authentication success to a user context profile. When a user goes online after a user authentication event authorization policy is applied to the device, the device adds the user to the context profile based on the user context identification result, and assigns the network access rights to the user based on the user authentication result.

Follow-up Procedure

1. In the user authentication event authorization policy view, run the **match access-context-profile action** command to configure the network access rights for users in each phase before authentication success.

2. In the system view, run the **access-author policy global** command to apply the user authentication event authorization policy.

Precautions

A maximum of two user authentication event authorization policies can be configured.

Example

Create the user authentication event authorization policy **a1**.

```
<HUAWEI> system-view
[HUAWEI] access-author policy name a1
```

13.5.6 access-domain

Function

The **access-domain** command configures a default or forcible domain in an authentication profile for users.

The **undo access-domain** command deletes a configured default or forcible domain in an authentication profile.

By default, no default or forcible domain is configured in an authentication profile.

Format

access-domain *domain-name* [**dot1x** | **mac-authen** | **portal**] * [**force**]

undo access-domain [**dot1x** | **mac-authen** | **portal**] * [**force**]

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name.	The value must be the name of an existing domain.
dot1x	Specifies a default or forcible domain for 802.1X authentication users.	-
mac-authen	Specifies a default or forcible domain for MAC address authentication users.	-
portal	Specifies a default or forcible domain for Portal authentication users.	-

Parameter	Description	Value
force	Specifies the configured domain as a forcible domain. If this parameter is not specified, the configured domain is a default domain.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device manages users in domains. For example, AAA schemes and authorization information are bound to domains. During user authentication, the device assigns users to specified domains based on the domain names contained in user names. However, user names entered by many users on actual networks do not contain domain names. In this case, you can configure a default domain in an authentication profile. If users using this profile enter user names that do not contain domain names, the device manages the users in the default domain.

On actual networks, user names entered by some users contain domain names and those entered by other users do not. The device uses different domains to manage the users. Because authentication, authorization and accounting (AAA) information in the domains are different, users use different AAA information. To ensure that users using the same authentication profile use the same AAA information, you can configure a forcible domain in the authentication profile for the users. The device then manages the users in the forcible domain regardless of whether entered user names contain domain names or not.

Prerequisites

A domain has been configured using the **domain** command in the AAA view.

Precautions

When you configure a default or forcible domain in an authentication profile, the domain takes effect as follows:

- If you do not specify the user authentication mode (**dot1x**, **mac-authen**, or **portal**), the domain takes effect for all access authentication users using the authentication profile.
- If both a default domain and a forcible domain are configured, the device authenticates users in the forcible domain.

- This function takes effect only for users who go online after this function is successfully configured.
- In a wireless scenario, RADIUS accounting is performed only for AAA users who do not need to pass authentication in a forcible domain, and cannot be performed for such users in the default domain.

Example

Configure the forcible domain **test** in the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] quit
[HUAWEI-aaa] quit
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] access-domain test force
```

13.5.7 access-user arp-detect

Function

The **access-user arp-detect** command sets the source IP address and source MAC address of offline detection packets in a VLAN.

The **undo access-user arp-detect** command deletes the source IP address and source MAC address of offline detection packets in a VLAN.

By default, the source IP address and source MAC address are not specified for offline detection packets in a VLAN.

Format

access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

undo access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
ip-address *ip-address*	Specifies the source IP address of offline detection packets.	The value is in dotted decimal notation and can be 0.0.0.0 or 255.255.255.255 or other valid IP address.

Parameter	Description	Value
mac-address *mac-address*	Specifies the source MAC address of offline detection packets.	The MAC address must be a unicast MAC address. The value is a hexadecimal number in the format H-H-H. Each H contains 1 to 4 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

If the VLAN to which the user belongs does not have a VLANIF interface or the VLANIF interface does not have an IP address, the device sends an offline detection packet using 0.0.0.0 as the source IP address. If a user cannot respond to an ARP probe packet with the source IP address 0.0.0.0, you can specify a source IP address for the offline detection packet.

In addition, a Windows client sends an ARP probe packet with the source IP address 0.0.0.0 after obtaining an IP address. In this case, if the device also sends an ARP probe packet with the source IP address 0.0.0.0, an IP address conflict occurs. In this case, you can specify an IP address as the source IP address of ARP probe packets sent by the device.

You are advised to specify the user gateway IP address and its corresponding MAC address as the source IP address and source MAC address of ARP probe packets sent by the device. If the gateway device changes, update the source MAC address of the ARP probe packets sent by the device in a timely manner. Otherwise, the gateway ARP entry on terminals may be incorrect, causing network disconnection.

Precautions

Only wired users support this function.

This function does not take effect for users who use Layer 3 Portal authentication.

For online users on physical interfaces, this command takes effect only after the users go online again or the device re-authenticates the users. For online users on Eth-Trunk interfaces, this command takes effect immediately.

The source IP or MAC addresses configured for offline detection packets using the following commands are listed in descending order of priority:

Example

Set the source IP address and MAC address of offline detection packets for users in VLAN 10 to 192.168.1.1 and 00e0-fc11-1234 respectively.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect vlan 10 ip-address 192.168.1.1 mac-address 00e0-fc11-1234
```

13.5.8 authentication arp-reply trigger

Function

The **authentication arp-reply trigger** command enables the function of triggering authentication by ARP response packets.

The **undo authentication arp-reply trigger** command disables the function of triggering authentication by ARP response packets.

By default, the function of triggering authentication by ARP response packets is enabled.

Format

authentication arp-reply trigger

undo authentication arp-reply trigger

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a client in sleep mode receives an ARP request packet, it replies with an ARP response packet, which triggers authentication. However, the authentication fails because no user name or password is entered when the client is in sleep mode. If the client is awakened before the re-authentication interval (specified by the **authentication timer re-authen authen-fail** *re-authen-time* command) expires, the user has to wait for a period of time before triggering authentication again. In this case, you can disable the function of triggering authentication by ARP response packets so that authentication is not triggered by ARP response packets sent by clients in sleep mode.

Precautions

This function is supported only for wired users.

When the function of triggering authentication by ARP packets is disabled, the function of triggering authentication by ARP response packets becomes ineffective.

The function of triggering authentication by ARP response packets takes precedence over the function of triggering authentication by any packets. When the function of triggering authentication by ARP response packets is disabled and the function of triggering authentication by any packets is enabled, authentication cannot be triggered by ARP response packets.

This function does not apply to MAC address authentication on VLANIF interfaces or Portal authentication.

Example

Enable the function of triggering authentication by ARP response packets.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication arp-reply trigger
```

13.5.9 access-user arp-detect default ip-address

Function

The **access-user arp-detect default ip-address** command sets the default source IP address of offline detection packets.

The **undo access-user arp-detect default ip-address** command restores the default setting.

By default, the default source IP address of offline detection packets is 0.0.0.0.

Format

access-user arp-detect default ip-address *ip-address*

undo access-user arp-detect default ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the default source IP address of offline detection packets.	The value is in dotted decimal notation and can be 0.0.0.0 or other valid IP address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

Precautions

- Only wired users support this function.
- This function does not take effect for users who use Layer 3 Portal authentication.
- In the SVF or policy association scenario, you are advised to run the **access-user arp-detect default ip-address** command to set the source IP address of offline detection packets to 0.0.0.0. In the SVF scenario, the command must be configured on the control device and takes effect only for control device detection. The default source IP address of offline detection packets for access device detection is 0.0.0.0. In the policy association scenario, you can directly configure the command on access devices.
- In normal situations, after a device sends an ARP probe packet with a default source IP address, online clients will immediately respond with ARP reply packets. If online clients do not respond with ARP reply packets, the device logs them out unexpectedly. To resolve this problem, use either of the following methods:
  - Run the **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address* command to specify a VLAN ID, source IP address, and source MAC address for ARP probe packets.
  - Run the **authentication timer handshake-period** *handshake-period* command to increase the handshake period so that the device can detect gratuitous ARP packets that these clients send at an irregular period. Once the device detects such packets, it does not log them out.
- The source IP or MAC addresses configured for offline detection packets using the following commands are listed in descending order of priority:
  - **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*
  - **access-user arp-detect fallback** *ip-address* { *mask* | *mask-length* }
  - **access-user arp-detect default ip-address** *ip-address*

  If two or more of the commands are configured, the source IP or MAC address with a higher priority takes effect.
- For online users on physical interfaces, this command takes effect only after the users go online again or the device re-authenticates the users. For online users on Eth-Trunk interfaces, this command takes effect immediately.

Example

Set the default source IP address of offline detection packets to 0.0.0.0.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect default ip-address 0.0.0.0
```


13.5.10 access-user dot1x-identity speed-limit

Function

The **access-user dot1x-identity speed-limit** command configures the rate limit of Identity packets for 802.1X authentication to be sent to the CPU.

The **undo access-user dot1x-identity speed-limit** command restores the default rate limit of Identity packets for 802.1X authentication to be sent to the CPU.

By default, the maximum of Identity packets for 802.1X authentication can be sent to the CPU every second depends on the device.

Format

access-user dot1x-identity speed-limit *value*

undo access-user dot1x-identity speed-limit [*value*]

Parameters

Parameter	Description	Value
value	Specifies the rate limit of Identity packets for 802.1X authentication to be sent to the CPU.	The value is an integer in the range of 5 to 2000, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a large number of Identity packets for 802.1X authentication are sent to the CPU of a switch, the CPU usage is high and other services are affected. To prevent this problem, run the **access-user dot1x-identity speed-limit** command to configure the rate limit of Identity packets for 802.1X authentication to be sent to the CPU, so that the switch discards excess Identity packets.

Example

Set the rate limit of Identity packets for 802.1X authentication to be sent to the CPU to 10 pps.

```
<HUAWEI> system-view
[HUAWEI] access-user dot1x-identity speed-limit 10
```


13.5.11 access-user arp-detect delay

Function

The **access-user arp-detect delay** command configures the delay in sending offline detection packets.

The **undo access-user arp-detect delay** command restores the default configuration.

By default, the delay in sending offline detection packets is 10 seconds.

Format

access-user arp-detect delay *delay*

undo access-user arp-detect delay

Parameters

Parameter	Description	Value
delay	Specifies the delay in sending offline detection packets.	The value is an integer in the range from 10 to 120, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A Windows client on the network sends a detection packet with the source address 0.0.0.0 after obtaining an IP address. If the device also initiates an ARP probe with the source address 0.0.0.0, a conflict occurs. To prevent this conflict, you can run the **access-user arp-detect delay** command to set the delay in sending offline detection packets. Typically, detection initiated by a Windows client takes 10 seconds. Therefore, a delay longer than 10 seconds is recommended.

Precautions

This function takes effect only for users who go online after it is configured.

This function takes effect in both ARP probe and ND probe scenarios.

NOTE

Delay after which the device sends the first ARP probe packet = Delay in sending offline detection packets + One-third of the handshake interval between the device and pre-connection or authorized users (configured using the **authentication timer handshake-period** command)

Example

Set the delay for sending offline detection packets to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect delay 20
```

13.5.12 access-user arp-detect fallback

Function

The **access-user arp-detect fallback** command configures an IP address required for calculating the source address of offline detection packets.

The **undo access-user arp-detect fallback** command deletes the IP address configured for calculating the source address of offline detection packets.

By default, no IP address is configured for the device to calculate the source address of offline detection packets.

Format

access-user arp-detect fallback *ip-address* { *mask* | *mask-length* }

undo access-user arp-detect fallback

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address required for calculating the source address of offline detection packets.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address.	The value is in dotted decimal notation. After the mask is converted into a binary number, all bits before the last 1 must be 1s. That is, 1s in the mask must be continuous and there cannot be any 0s before the last 1.
mask-length	Specifies the mask length of the IP address.	The value is an integer in the range from 0 to 32.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device does not function as a gateway, it can send offline detection packets with the source address on the same network segment as clients. This source address is calculated based on the client network segment and the IP address specified in the **access-user arp-detect fallback** command. The operation AND is performed between this specified IP address and the wildcard mask to obtain result 1. Then result 1 is added to the network segment of clients to get the source address of offline detection packets. For example, if the network segment of clients is 192.168.1.0/24 and **access-user arp-detect fallback 0.0.0.11 24** is configured, the source address of offline detection packets is 192.168.1.11. The calculated source address must be excluded from the address pool of the DHCP server to prevent IP address conflicts.

Precautions

Only wired users support this function.

This function does not take effect for users who use Layer 3 Portal authentication.

For online users on physical interfaces, this command takes effect only after the users go online again or the device re-authenticates the users. For online users on Eth-Trunk interfaces, this command takes effect immediately.

- The source IP or MAC addresses configured for offline detection packets using the following commands are listed in descending order of priority:
  - **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*
  - **access-user arp-detect fallback** *ip-address* { *mask* | *mask-length* }
  - **access-user arp-detect default ip-address** *ip-address*

  If two or more of the commands are configured, the source IP or MAC address with a higher priority takes effect.

Example

Set the IP address required for calculating the source address of offline detection packets to 0.0.0.11.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect fallback 0.0.0.11 24
```


13.5.13 access-user car-mode

Function

The **access-user car-mode** command configures the CAR mode for user access.

The **undo access-user car-mode** command restores the CAR mode for user access to **default**.

By default, the CAR mode for user access is **default**.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

access-user car-mode { **dual-stack** | **default** }

undo access-user car-mode

Parameters

Parameter	Description	Value
dual-stack	Specifies this CAR mode in scenarios where there are only wired or wireless dual-stack users on the network and authorization and accounting are performed on these users.	When this mode is specified, the rate limits are adjusted for the following types of packets: 8021x-start, 8021x-identity, nac-arp-request, capwap-association, capwap-disassoc, nac-nd, and nac-dhcpv6.
default	Specifies the default CAR mode in scenarios where authorization or accounting is not performed on users.	When this mode is specified, the system restores the default rate limits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the CAR mode for user access is **default**. This mode applies to scenarios where user authentication is performed but user authorization or accounting is not performed. In this mode, users can be quickly authenticated and go online.

When the device connects to the iMaster NCE-Campus controller, the controller delivers some authorization, accounting, and device and user statistics reporting configurations to the device by default, affecting the CPU usage of the device. To reduce the CPU load on the device, you need to adjust the user access rate. For example:

- When the device is deployed at the core layer and functions as the access authentication point for wireless users, you can specify **dual-stack** based on whether IPv6 users exist.
- When the device is deployed at the access or aggregation layer and functions as the access authentication point for wired users, you can specify **dual-stack** based on whether IPv6 users exist.

After the CAR mode for user access is configured, you can run the **display cpu-defend configuration** command to query the rate limits of packets.

Precautions

If the rate limits of specific packet types adjusted by this command conflict with those adjusted by the **car (attack defense policy view)** command, the rate limits adjusted by the **car (attack defense policy view)** command take effect.

Example

Set the CAR mode for user access to **dual-stack**.

```
<HUAWEI> system-view
[HUAWEI] access-user car-mode dual-stack
```

13.5.14 access-user https speed-limit

Function

The **access-user https speed-limit** command sets the limit of the rate at which HTTPS protocol packets are sent to the CPU.

The **undo access-user https speed-limit** command restores the default limit of the rate at which HTTPS protocol packets are sent to the CPU.

By default, the limit of the rate at which HTTPS protocol packets are sent to the CPU depends on the device model.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

access-user https speed-limit *value*

undo access-user https speed-limit [*value*]

Parameters

Parameter	Description	Value
value	Specifies the rate limit.	The value is an integer in the range from 3 to 2000, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a switch processes two many HTTPS protocol packets, the CPU usage may become high and other services are affected. To address this issue, run the **access-user https speed-limit** command to set the limit of the rate at which HTTPS protocol packets are sent to the CPU. If the rate at which HTTPS protocol packets are sent to the CPU exceeds the specified value, the switch discards the excessive HTTPS protocol packets.

Example

Set the limit of the rate at which HTTPS protocol packets are sent to the CPU to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] access-user https speed-limit 50
```

13.5.15 access-user portal speed-limit

Function

The **access-user portal speed-limit** command sets the limit of the rate at which Portal protocol packets are sent to the CPU.

The **undo access-user portal speed-limit** command restores the default limit of the rate at which Portal protocol packets are sent to the CPU.

By default, the limit of the rate at which Portal protocol packets are sent to the CPU depends on the device model.

Format

access-user portal speed-limit *value*

undo access-user portal speed-limit [*value*]

Parameters

Parameter	Description	Value
value	Specifies the rate limit.	The value is an integer in the range from 5 to 2000, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a switch processes two many Portal protocol packets, the CPU usage may become high and other services are affected. To address this issue, run the **access-user portal speed-limit** command to set the limit of the rate at which Portal protocol packets are sent to the CPU. If the rate at which Portal protocol packets are sent to the CPU exceeds the specified value, the switch discards the excessive Portal protocol packets.

Example

Set the limit of the rate at which Portal protocol packets are sent to the CPU to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] access-user portal speed-limit 50
```

13.5.16 access-user syslog-restrain enable

Function

The **access-user syslog-restrain enable** command enables system log suppression.

The **undo access-user syslog-restrain enable** command disables system log suppression.

By default, system log suppression is enabled.

Format

access-user syslog-restrain enable

undo access-user syslog-restrain enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a user fails in authentication or goes offline, the device records a system log. The system log contains the MAC addresses of access device and access user and the authentication time.

If a user repeatedly attempts to go online after authentication failures or frequently goes online and offline in a short period, a lot of system logs are generated, which waste system resources and degrade system performance. System log suppression can address this problem. After the device generates a system log, it will not generate the same log within the suppression period (set by **access-user syslog-restrain period**).

NOTE

The same system logs refer to the system logs containing the same MAC addresses. For example, after the device generates a system log for a user failing in authentication, the device will not generate new system log for this user in the suppression period if the user fails in authentication again. The system logs for users logging offline are generated in the same way. If a system log has no MAC address, such system logs are suppressed based on the user name.

Example

Enable system log suppression.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain enable
```

13.5.17 access-user syslog-restrain period

Function

The **access-user syslog-restrain period** command sets a period for system log suppression.

The **undo access-user syslog-restrain period** command restores the default period for system log suppression.

By default, the period of system log suppression is 300s.

Format

access-user syslog-restrain period *period*

undo access-user syslog-restrain period

Parameters

Parameter	Description	Value
period	Specifies the period for system log suppression.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the system log suppression function is enabled using the **access-user syslog-restrain enable** command, use this command to set the system log suppression period. After generating a system log, the device will not generate the same log within the suppression period.

Example

Set the period for system log suppression to 600s.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain period 600
```

13.5.18 acl authorization statistics enable

Function

The **acl authorization statistics enable** command enables statistics collection on packets that match the ACLs assigned for authorization.

The **undo acl authorization statistics enable** command disables statistics collection on packets that match the ACLs assigned for authorization.

By default, statistics collection on packets that match the ACLs assigned for authorization is disabled.

Format

acl authorization statistics enable

undo acl authorization statistics enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a live network, the authentication server may assign ACLs to users who pass NAC authentication to grant the users access to the network. You can run the **acl authorization statistics enable** command to check the number of user packets that match the assigned ACLs.

Precautions

The function takes effect only for users who go online after this function is enabled, and for the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, and S5720-LI, this function cannot be used to collect statistics on packets that match the permit rules in redirection ACLs.

Example

Enable statistics collection on packets that match the ACLs assigned for authorization.

```
<HUAWEI> system-view
[HUAWEI] acl authorization statistics enable
```

13.5.19 acl-id (service scheme view)

Function

The **acl-id** command binds an ACL to a service scheme.

The **undo acl-id** command unbinds the ACL from the service scheme.

By default, no ACL is bound to a service scheme.

Format

acl-id [**ipv6**] *acl-number*

undo acl-id { [**ipv6**] *acl-number* | **all** }

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1, S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S6720-EI, S6735-S, , S6720S-EI support the **ipv6** parameter.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL bound to a service scheme.	The ACL number for wired users ranges from 3000 to 3999. The ACL number for wireless users ranges from 3000 to 3999 in tunnel forwarding mode, or from 3000 to 3031 in direct forwarding mode. **NOTE** In terms of authorization ACLs configured on a server, the ACL number for wired users ranges from 2000 to 3999, and the redirect ACL number ranges from 3000 to 3999; the ACL number for wireless users ranges from 2000 to 3999 in tunnel forwarding mode, or from 3000 to 3031 in direct forwarding mode.
ipv6	Indicates that the ACL bound to a service scheme is an IPv6 ACL. If this parameter is not specified, the ACL bound to a service scheme is an IPv4 ACL.	The IPv6 ACL number ranges from 3000 to 3999.
all	Deletes the numbers of all ACLs bound to a service scheme.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme** command, you can run the **acl-id** command to bind an ACL to the service scheme. The user assigned with the service scheme will have the ACL rules.

Prerequisites

An IPv4 ACL must have been created using the **acl** or **acl name** command.

An IPv6 ACL has been created using the **acl ipv6** or **acl ipv6 name** command.

Precautions

If the ACL authorized to users who go online through S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S is not a user-defined one, the attribute of the source IP address in the ACL rule does not take effect. In all other cases, the IP address in the ACL rule is replaced with the user's IP address. The IP address in the ACL rule will be replaced with the user's IP address.

Number of ACLs that can be bound to a service scheme:

- S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: 1. If you run this command multiple times, only the latest configuration takes effect.
- The other models: 4

The maximum number of IPv6 ACLs that can be bound to a service scheme is 1. If you run this command multiple times, only the latest configuration takes effect.

In the policy association scenario, if multiple ACLs are configured using this command on the authentication control device, only the first configured one takes effect on the authentication access device.

An ACL can be configured with a maximum of 129 rules. In wireless scenarios If the rule specification contains a matching port range (destination-port range or source-port range), extra hardware resources are occupied. As a result, the maximum number of rules cannot be delivered.

Ensure that the bound ACL has been created. Otherwise, ACL authorization fails for users who go online through the service scheme, and users may fail to go online.

Example

Bind ACL 3001 to the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] acl-id 3001
```

13.5.20 authentication handshake

Function

The **authentication handshake** command enables the handshake with pre-connection users and authorized users.

The **undo authentication handshake** command disables the handshake with pre-connection users and authorized users.

By default, the handshake with pre-connection users and authorized users is enabled.

Format

authentication handshake

undo authentication handshake

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device creates entries for pre-connection users, users who fail to be authenticated and are assigned network access rights, and users who are authenticated. After users go offline in normal situations, the system immediately deletes the corresponding user entries. However, if some users go offline due to exceptions such as network disconnections, the system cannot immediately delete the corresponding user entries. If there are too many such user entries, other users may fail to access the network.

To solve this problem, run the **authentication handshake** command to enable the handshake with pre-connection users and authorized users. If a user does not respond to the handshake request from the device within the handshake interval, the device deletes the user entry.

Precautions

- The handshake interval for MAC address authentication users, Layer 3 Portal authentication users, and 802.1X authentication users is configured using the **authentication timer handshake-period** command. The handshake interval for Layer 2 Portal authentication users is configured using the **portal timer offline-detect** command.
- For Layer 3 Portal authentication users, only those who go online through S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this function.
- This function takes effect only for wired users. For users without IP addresses, the device sends probe packets after a delay of 30 minutes. If the device receives no reply packet from such users within a handshake interval, it logs out the users.

- When the configuration changes, the configuration takes effect only for new online wired users.
- The handshake function is implemented using ARP probe packets or neighbor discovery (ND) probe packets.
- The handshake function can also be implemented by detecting whether there is user traffic on the access device. Assuming that the handshake interval is **3n**, the device will detect user traffic at **n** and **2n**. The following uses the **0-n** period as an example. The process during the **n-2n** period is similar to that during **0-n**. (This process applies only to authentication users who go online from the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI. Other switch models do not detect user traffic and send probe packets at **n** and **2n**.)
  - If user traffic passes the device during the **0-n** period, the device considers that the user is online at **n**, so it will not send a probe packet to the user, but resets the handshake interval.
  - If no user traffic passes the device during the **0-n** period, the device cannot determine whether the user is online at **n**, so it sends a probe packet to the user. If the device receives the reply packet from the user, it considers the user online and resets the handshake interval. If no reply packet is received, it considers the user offline.
  - If user traffic passes the device during the **2n-3n** period, the device considers that the user is online at **3n** and resets the handshake interval.
  - If no user traffic passes the device during the **2n-3n** period, the device cannot determine whether the user is online at **3n** and considers that the user is offline.

  If the device considers that the user is offline at **n**, **2n**, and **3n**, the device deletes all entries related to the user. To prevent the user from going offline unexpectedly when no operation is performed on the PC, do not set a short handshake period.

Example

In the authentication profile **p1**, enable the handshake with pre-connection users and authorized users.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication handshake
```

13.5.21 authentication control-direction

Function

The **authentication control-direction** command configures the direction of traffic controlled by the device.

By default, the device only controls the upstream traffic.

Format

authentication control-direction { **all** | **inbound** }

Parameters

Parameter	Description	Value
all	Configures bidirectional traffic control.	-
inbound	Controls only the upstream traffic.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the access authentication device discards all the traffic sent from the users who fail the 802.1x authentication or MAC address authentication. However, these users can still receive packets broadcast from network devices to successfully authenticated users in the same VLAN. To disable the users who fail the authentication from receiving the broadcast packets, run the **authentication control-direction all** command to configure bidirectional traffic control. To restore the default situation, run the **authentication control-direction inbound** command so that the device only controls the traffic sent from the users who fail the authentication.

Precaution

- This function applies only to 802.1x authentication and MAC address authentication.
- This function takes effect only when an access switch functions as the authentication device and an interface of the switch is connected to only one IP phone or PC.
- This function does not take effect when users have pre-connection entries or authentication event entries. You are advised to run the **undo authentication pre-authen-access enable** command disable the function of keeping users who fail to be authenticated and do not have any network access rights in the pre-connection state, and do not run the **authentication event** command to configure the device to assign network access rights to users in each phase before authentication succeeds.
- When there are both successfully authenticated users and users who fail to be authenticated on the same interface in the same VLAN, bidirectional traffic control does not take effect on this interface.
- Layer 3 interfaces do not support bidirectional traffic control.
- You are advised to run the **stp edged-port enable** command to configure the interface on which the function is applied as an edge port. The interface can be added to a maximum of four VLANs.

- The SVF and policy association scenarios do not support this function.
- WLAN scenarios do not support this function.
- When this function is configured, the recommended STP mode is VBST. If the STP mode is changed after users go online, traffic will be interrupted for a short time. If the STP mode is set to MSTP or STP, run the **instance** command to map VLANs to different spanning tree instances (MSTIs).
- A user VLAN cannot be specified as an RRPP or ERPS control VLAN.
- After bidirectional traffic control is configured using the **authentication control-direction all** command, authentication can still be triggered even if a loop occurs on the downstream interface.

Example

Configure bidirectional traffic control in the authentication profile **authen1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication control-direction all
```

13.5.22 authentication device-type voice authorize

Function

The **authentication device-type voice authorize** command enables voice terminals to go online without authentication.

The **undo authentication device-type voice authorize** command disables voice terminals from going online without authentication.

By default, voice terminals are disabled from going online without authentication.

Format

authentication device-type voice authorize [**service-scheme** *scheme-name*]

undo authentication device-type voice authorize [**service-scheme**]

Parameters

Parameter	Description	Value
service-scheme *scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to voice terminals.	The value must be an existing service scheme name.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both data terminals (such as PCs) and voice terminals (such as IP phones) are connected to devices, NAC is configured on the devices to manage and control the data terminals. The voice terminals, however, only need to connect to the network without being managed and controlled. In this case, you can configure the voice terminals to go online without authentication on the devices. Then the voice terminals identified by the devices can go online without authentication.

Precautions

When a RADIUS server is used for dynamic VLAN delivery, the following RADIUS attributes must be used: (064) Tunnel-Type (which must be set to VLAN or 13), (065) Tunnel-Medium-Type (which must be set to 802 or 6), and (081) Tunnel-Private-Group-ID (which can be set to the VLAN ID, VLAN description, VLAN name, or VLAN pool). To ensure that the RADIUS server delivers VLAN attributes correctly, all the three RADIUS attributes must be used. In addition, the Tunnel-Type and Tunnel-Medium-Type attributes must be set to the specified values. When a voice VLAN is delivered, the RADIUS attribute (26-33) HW-Voice-Vlan must also be used.

To enable the switches to identify the voice terminals, enable LLDP or configure OUI for the voice VLAN on the switches. For details, see "Configuring Basic LLDP Functions" in "LLDP Configuration" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Network Management and Monitoring* or "Configuring a Voice VLAN Based on a MAC Address" in "Voice VLAN Configuration" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Ethernet Switching*. If a voice device supports only CDP but does not support LLDP, configure CDP-compatible LLDP on the switch using **lldp compliance cdp receive** command.

After the voice VLAN function is enabled on an interface using the **voice-vlan enable** command, authenticated voice terminals are authorized to use the voice VLAN if the VLAN of the voice terminals is the same as the voice VLAN.

If an 802.1X user initiates authentication through a voice terminal, a device preferentially processes the authentication request. If the authentication succeeds, the terminal obtains the corresponding network access rights. If the authentication fails, the device identifies the terminal type and enables the terminal to go online without authentication.

If you run this command repeatedly, the latest configuration overrides the previous ones.

This function takes effect only for users who go online after this function is successfully configured.

When voice terminals access the network without authentication, accounting is not supported.

Example

In the authentication profile **p1**, enable the device to allow voice terminals to go online without authentication and assign the service scheme **s1** to voice terminals that are not authenticated.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] quit
[HUAWEI-aaa] quit
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication device-type voice authorize service-scheme s1
```

13.5.23 authentication device-type iconnect authorize

Function

The **authentication device-type iconnect authorize** command enables iConnect terminals to go online without being authenticated.

The **undo authentication device-type iconnect authorize** command disables iConnect terminals from going online without being authenticated.

By default, iConnect terminals cannot go online without being authenticated.

NOTE

Only S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

authentication device-type iconnect authorize [**service-scheme** *scheme-name*]

undo authentication device-type iconnect authorize [**service-scheme**]

Parameters

Parameter	Description	Value
service-scheme *scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to iConnect terminals.	The value must be the name of an existing service scheme.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

iConnect is the name of an ecosystem at the network layer in the CloudCampus Solution. iConnect terminals refer to IoT terminals that use the iConnect ecosystem. NAC is required for most terminals, but not iConnect terminals. To enable iConnect terminals to go online without being authenticated, run the **authentication device-type iconnect authorize** command.

Precautions

This function takes effect only for MAC address authentication and Portal authentication users in wireless scenarios. This function cannot be configured in MAC+802.1X authentication scenarios.

This function has a higher priority than pre-connection authorization and authorization upon authentication failures.

This function does not take effect for open users.

If you run this command multiple times, only the latest configuration takes effect.

This function takes effect only for users who go online after this function is successfully configured.

Example

In the authentication profile **p1**, enable the device to allow iConnect terminals to go online without authentication and assign the service scheme **s1** to iConnect terminals that are not authenticated.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] quit
[HUAWEI-aaa] quit
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication device-type iconnect authorize service-scheme s1
```

13.5.24 authentication dot1x-mac-bypass

Function

The **authentication dot1x-mac-bypass** command enables MAC address bypass authentication.

The **undo authentication dot1x-mac-bypass** command disables MAC address bypass authentication.

By default, MAC address bypass authentication is disabled.

Format

authentication dot1x-mac-bypass

undo authentication dot1x-mac-bypass

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure MAC address bypass authentication to authenticate terminals such as printers that cannot have the 802.1X client installed.

After MAC address bypass authentication is enabled in an authentication profile, the device performs 802.1X authentication for users using the authentication profile. If the user name request times out, the device starts the MAC address authentication process for the users.

Precautions

MAC address bypass authentication involves 802.1X authentication and MAC address authentication. Before enabling this function in an authentication profile, ensure that an 802.1X access profile and a MAC access profile have been bound to the authentication profile.

Example

In the authentication profile **p1**, enable MAC address bypass authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication dot1x-mac-bypass
```

13.5.25 authentication drop dhcp-packet user-no-online enable

Function

The **authentication drop dhcp-packet user-no-online enable** command enables a device to discard DHCP packets when an 802.1X authentication user is offline or being re-authenticated.

The **undo authentication drop dhcp-packet user-no-online enable** command disables a device from discarding DHCP packets when an 802.1X authentication user is offline or being re-authenticated.

By default, the device does not discard DHCP packets when an 802.1X authentication user is offline or being re-authenticated.

Format

authentication drop dhcp-packet user-no-online enable

undo authentication drop dhcp-packet user-no-online enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios where MAC address + 802.1X authentication is configured, the device permits DHCP Request packets from an 802.1X client and replies with DHCP ACK packets even when 802.1X authentication fails. In this case, the client failing the 802.1X authentication can still obtain an IP address through DHCP. As a result, the DHCP process is not triggered during subsequent MAC address authentication. To resolve this problem, you can run the **authentication drop dhcp-packet user-no-online enable** command to enable the device to discard DHCP and DHCPv6 packets when an 802.1X authentication user is offline or being re-authenticated. In this way, the DHCP process can be triggered when MAC address authentication is performed after an 802.1X authentication failure.

Prerequisites

An 802.1X access profile has been bound to an authentication profile.

Precautions

1. When the **authentication drop dhcp-packet user-no-online enable** command is configured in the VLANIF interface view where authentication is enabled, the configuration does not take effect.
2. When the **authentication drop dhcp-packet user-no-online enable** command is configured and DHCP packets match an authentication-free rule, the authentication-free rule preferentially takes effect; that is, DHCP packets are forwarded or discarded according to the authentication-free rule.

Example

Enable the device to discard DHCP packets when an 802.1X authentication user is offline or being re-authenticated in the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication drop dhcp-packet user-no-online enable
```


13.5.26 authentication event action authorize

Function

The **authentication event action authorize** command configures authentication event authorization information.

The **undo authentication event action authorize** command restores the default setting.

By default, authentication event authorization information is not configured.

Format

User authorization in the case of pre-connections:

authentication event pre-authen action authorize { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* }

undo authentication event pre-authen action authorize

User authorization when authentication fails:

authentication event authen-fail action authorize { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* } [**response-fail**]

undo authentication event authen-fail action authorize

User authorization when the authentication server is Down:

authentication event authen-server-down action authorize { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* } [**response-fail**]

authentication event authen-server-down action authorize keep [**no-response** | **response-fail**]

undo authentication event authen-server-down action authorize

User authorization when the authentication server does not respond:

authentication event authen-server-noreply action authorize keep [**no-response** | **response-fail**]

undo authentication event authen-server-noreply action authorize

Parameters

Parameter	Description	Value
pre-authen	Configures the device to assign network access rights to users when the users establish pre-connections with the device.	-

Parameter	Description	Value
authen-fail	Configures the device to assign network access rights to users when the authentication server sends authentication failure packets to the device.	-
authen-server-down	Configures the device to assign network access rights to users when the authentication server is Down or the server is in the forcible Up state.	-
authen-server-noreply	Configures the device to assign network access rights to users when the authentication server does not respond.	-
response-fail	Configures the device to send authentication failure packets to users after assigning network access rights to the users. If this parameter is not specified, the device by default sends authentication success packets to users and therefore the users cannot know the fact that they fail to be authenticated. To solve this problem, specify this parameter so that the device will send authentication failure packets for the users to know their authentication results. **NOTE** When both the **authentication event authen-server-down action authorize** and **authentication event authen-server-down action authorize keep** commands are configured and the **response-fail** parameter is specified, both commands take effect.	-

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID. When this parameter is specified, users can access only the resources in the VLAN.	The value is an integer that ranges from 1 to 4094. The VLAN must exist on the device. Otherwise, the configuration does not take effect.
service-scheme *service-scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to users.	The value must be an existing service scheme name on the device.
ucl-group *ucl-group-name*	Specifies the name of the UCL group based on which network access rights are assigned to users.	The value must be an existing UCL group name on the device.
keep	Configures online uses to retain original network access rights. **NOTE** If an online user is re-authenticated in a different authentication mode from the original one, the online user cannot retain the original network access permissions.	-
no-response	Configures the device not to send response packets to users after assigning network access rights to the users. If this parameter is not specified, the device sends an authentication success packet to users.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If users establish pre-connections with the device or fail to be authenticated, they have no network access rights.

To meet these users' basic network access requirements such as updating the antivirus database and downloading a client, configure authentication event authorization information. The device will assign network access rights to these users based on the user authentication phase.

Precautions

Wireless 802.1X authentication only supports the **keep** parameter.

If no network access right is configured for users who fail authentication or when the authentication server is Down, the users establish pre-connections with the device after the authentication fails and then have the network access rights mapping pre-connection users.

VLAN-based authorization does not apply to the authentication users who access through VLANIF interfaces.

To use VLAN-based authorization (excluding authentication of pre-connection users), run the **undo authentication pre-authen-access enable** command to disable the pre-connection function first.

An authorized VLAN cannot be delivered to online Portal users.

If a user uses Portal authentication, the **keep** parameter cannot be configured.

The configured **vlan**, **service-scheme**, or **ucl-group** parameter takes effect only for new online users.

For S6720-EI, S6720S-EI, if the user upstream rate limit is configured in the QoS profile bound to a service scheme, do not configure the device to use the service scheme to grant network access rights to users in the pre-connection phase. Otherwise, users go offline.

When the authentication server is in Down state, user authentication fails, or the user is in pre-connection state, the redirect ACL function is not supported. For details about this function, see **redirect-acl**.

In 802.1X authentication for wired users, when the RADIUS server is Down, some new clients do not have escape rights. For example, when a new Windows client receives a Success packet from the device but does not receive the authentication packets exchanged with the RADIUS server, the client will fail the authentication and cannot go online. Currently, the following clients have escape rights when they go online for the first time: H3C iNode clients using EAP-MD5 or PEAP and Cisco AnyConnect clients using EAP-FAST or PEAP. For Windows clients, for example, Windows 7, choose "Local Area Connection> Properties> Authentication> Fallback to unauthorized network access".

Authentication event authorization information cannot be configured for static users identified by IP addresses.

If Portal authentication has been configured, VLAN-based authorization used when the authentication server is Down or configured for users who are in pre-connection state or fail the authentication does not take effect.

Example

In the authentication profile **authen1**, configure the device to assign network access rights specified in VLAN 10 to pre-connection users.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication event pre-authen action authorize vlan 10
```

13.5.27 authentication event authen-server-down action close re-authen

Function

The **authentication event authen-server-down action close re-authen** command disables re-authentication when the authentication server is Down.

The **undo authentication event authen-server-down action close re-authen** command restores the default setting.

By default, re-authentication is enabled when the authentication server is Down.

Format

authentication event authen-server-down action close re-authen

undo authentication event authen-server-down action close re-authen

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

In a re-authentication scenario, after the **authentication event action authorize keep** command is run, online users retain the original network access rights when the authentication server is Down. If re-authentication is performed on these users, the client frequently initiates re-authentication and may remain silent after multiple times. As a result, these users cannot access the network. To prevent this problem, you are advised to run the **authentication event authen-server-down action close re-authen** command to disable re-authentication when the authentication server is Down.

Example

Disable re-authentication when the authentication server is Down.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication event authen-server-down action close re-authen
```

13.5.28 authentication event authen-server-up action re-authen

Function

The **authentication event authen-server-up action re-authen** command enables the device to re-authenticate users in the survival state when the authentication server changes from Down or forcible Up to Up.

The **undo authentication event authen-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users in the survival state when the authentication server changes from Down or forcible Up to UP.

Format

authentication event authen-server-up action re-authen

undo authentication event authen-server-up action re-authen

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The users in the survival state can only access limited network resources after the device assigns specified network access rights to users who fail authentication because the authentication server is Down. To meet the users' normal network access requirements, the device needs to re-authenticate users in the survival state in real time when the authentication server turns Up.

After the status of the RADIUS server is set to Down, you can run the **radius-server dead-time** *dead-time* command to set the interval for the RADIUS server to return to the active state. When the value of *dead-time* expires, the status of the RADIUS server is set to forcible Up. When the server successfully transmits and

receives packets, the status is set to Up. The device can re-authenticate users in the survival state when the server changes from Down or forcible Up to Up. Re-authentication cannot be triggered when the server turns from Down to forcible Up.

Prerequisites

The **radius-server testuser** command has been configured in the RADIUS server template so that the device can detect that the authentication server changes from Down to Up.

Example

In the authentication profile **authen1**, enable the device to re-authenticate users when the authentication server turns Up from Down or forcible Up.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication event authen-server-up action re-authen
```

13.5.29 authentication event client-no-response action authorize

Function

The **authentication event client-no-response action authorize** command configures network access rights for users when the 802.1X client does not respond.

The **undo authentication event client-no-response action authorize** command restores the default setting.

By default, no network access right is configured for users when the 802.1X client does not respond.

Format

authentication event client-no-response action authorize { **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* | **vlan** *vlan-id* }

undo authentication event client-no-response action authorize

Parameters

Parameter	Description	Value
service-scheme *service-scheme-name*	Specifies the name of a service scheme based on which network access rights are assigned.	The value must be an existing service scheme name on the device.

Parameter	Description	Value
ucl-group *ucl-group-name*	Specifies the name of a UCL group based on which network access rights are assigned.	The value must be an existing UCL group name on the device.
vlan *vlan-id*	Specifies a VLAN ID. When this parameter is specified, users can access only the resources in the VLAN.	The value is an integer that ranges from 1 to 4094.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the 802.1X client does not respond, users cannot pass authentication and thereby have no network access right. Before being successfully authenticated, some users may need certain basic network access rights to download client software and update the antivirus database. The network access rights can be configured for the users when the 802.1X client does not respond, so that the users can access specified network resources.

Precautions

Wireless 802.1X authentication does not support this function.

This function takes effect only for users who go online after this function is successfully configured.

When an 802.1X client does not respond, the redirect ACL function is not supported. For details about the function, see **redirect-acl**.

In multi-mode authentication mode, if the function of assigning network access rights to users when the 802.1X client does not respond, the user status changes between Pre-authen and Client-no-resp, causing the function not to take effect.

Example

In the 802.1X access profile **d1**, configure the device to assign the network access rights specified in VLAN 10 for users when the 802.1X client does not respond.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] authentication event client-no-response action authorize vlan 10
```


13.5.30 authentication event portal-server-down action authorize

Function

The **authentication event portal-server-down action authorize** command configures network access rights for users when the Portal server is Down.

The **undo authentication event portal-server-down action authorize** command deletes the network access rights configured for users when the Portal server is Down.

By default, no network access right is configured for users when the Portal server is Down.

Format

authentication event portal-server-down action authorize { **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* }

undo authentication event portal-server-down action authorize

Parameters

Parameter	Description	Value
service-scheme *service-scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to users.	The value must be an existing service scheme name.
ucl-group *ucl-group-name*	Specifies the name of the UCL group based on which network access rights are assigned to users.	The value must be an existing UCL group name.

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the Portal server is Down, users cannot pass the authentication and thereby have no network access right. Before being successfully authenticated, some users may need certain basic network access rights to download client software and update the antivirus database. The network access rights can be configured for

the users when the Portal server is Down, so that the users can access specified network resources.

Prerequisites

A UCL group has been created using the **ucl-group** command in the system view.

A service scheme has been created using the **service-scheme** command in the AAA view.

Precautions

- This function takes effect only for users who go online after this function is successfully configured.
- This function is not supported in Policy Association scenarios.
- Only HTTP/HTTPS messages-triggered portal authentication users support this function.
- Before enabling the access device to assign network access rights to users when the Portal server is Down, enable the heartbeat detection function on the Portal server and run the **server-detect** command on the access device to enable the Portal server detection function.
- When the Portal server is in Down state, the redirect ACL function is not supported. For details about this function, see **redirect-acl**.
- When both the network access permission and user authentication failure authorization are configured, and the user fails to be authenticated. If the Portal Server Down message is triggered, the user obtains the network access permission when the Portal server is Down. If the Portal Server Down message is not triggered, the user obtains the network access permission

Example

In the Portal access profile **p1**, configure the device to assign network access rights based on the service scheme **s1** to users when the Portal server is Down.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] quit
[HUAWEI-aaa] quit
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] authentication event portal-server-down action authorize service-scheme s1
```

13.5.31 authentication event portal-server-up action re-authen

Function

The **authentication event portal-server-up action re-authen** command enables the device to re-authenticate users when the Portal server turns Up from Down.

The **undo authentication event portal-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users when the Portal server turns Up from Down.

Format

authentication event portal-server-up action re-authen

undo authentication event portal-server-up action re-authen

Parameters

None

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is configured to assign network access rights to users when the Portal server is Down, users can access limited network resources after the device detects that the Portal server is Down. To ensure that users can obtain normal network access rights after the Portal server goes Up, you can enable the device to re-authenticate users when the Portal server changes from Down to Up. After the Portal server goes Up, the device sets the status of users who display **web-server-down** to pre-connection. The re-authentication process starts when the users visit any web page. If the authentication succeeds, the device assigns normal network access rights to the users.

Precautions

- This command does not apply to users connected to the route main interface.
- This function takes effect only for users who go online after this function is successfully configured.
- Before enabling the access device to assign network access rights to users when the Portal server is Down, enable the heartbeat detection function on the Portal server and run the **server-detect** command on the access device to enable the Portal server detection function.

Example

In the Portal access profile **p1**, enable the device to re-authenticate users when the Portal server turns Up from Down.

```
<HUAWEI> system-view
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] authentication event portal-server-up action re-authen
```


13.5.32 authentication https-redirect enable

Function

The **authentication https-redirect enable** command enables HTTPS redirection for Portal or 802.1X authentication.

The **undo authentication https-redirect enable** command disables HTTPS redirection for Portal or 802.1X authentication.

By default, HTTPS redirection for Portal or 802.1X authentication is enabled.

Format

authentication https-redirect enable

undo authentication https-redirect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Portal authentication scenarios, many well-known websites, such as Google and Baidu, use HTTPS. When a user accesses an HTTPS website, the user must be redirected to the Portal authentication page so that the user can be authenticated and access the Internet. After HTTPS redirection for Portal authentication is enabled, the device redirects unauthenticated Portal users to the Portal authentication page when they access HTTPS websites.

In 802.1X or Portal authentication scenarios, if the web page push function is deployed for HTTPS packets, run the **authentication https-redirect enable** command to enable the HTTPS redirection function. Otherwise, the web page push function does not take effect.

Precautions

- When Portal authentication is triggered while a user accesses an HTTPS website, the browser displays a security prompt, requiring the user to click **Continue** to complete Portal authentication.
- Redirection is not supported if the browser or website runs HTTP Strict Transport Security (HSTS).
- If the destination port number of the HTTPS request packet sent by the user is not a well-known port number (443), redirection cannot be performed.

- To enable HTTPS redirection of Portal authentication for wired Portal authentication users, run the **authentication https-redirect enable** command, and then run the **portal https-redirect wired enable** command.
- This function takes effect only for new Portal or 802.1X authentication users.
- For the S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S500, S5735-S-I, the user access rate of the HTTPS redirection function is low. Therefore, this function is not recommended when a large number of users go online.

Example

Enable HTTPS redirection for Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication https-redirect enable
```

13.5.33 authentication ip-address in-accounting-start

Function

The **authentication ip-address in-accounting-start** command enables the function of carrying users' IP addresses in Accounting-Start packets.

The **undo authentication ip-address in-accounting-start** command disables the function of carrying users' IP addresses in Accounting-Start packets.

By default, the function of carrying users' IP addresses in Accounting-Start packets is enabled.

Format

authentication ip-address in-accounting-start

undo authentication ip-address in-accounting-start

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device reports access information and basic network information (IP address) of users through Accounting-Start packets. Therefore, the device needs to support carrying users' IP addresses in Accounting-Start packets.

Precautions

If the device cannot learn IP addresses of users, the device does not send Accounting-Start packets.

This command takes effect only for 802.1X authentication and MAC address authentication users. By default, Accounting-Start packets for Portal authentication carry users' IP addresses.

This command takes effect on both IPv4 and IPv6 users. You can run the **authentication ipv4-address in-accounting-start mandatory** command to configure the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets.

In the earlier V200R020C10 versions, the function of carrying users' IP addresses in Accounting-Start packets is disabled by default. In the V200R020C10 and later versions, the function of carrying users' IP addresses in Accounting-Start packets is enabled by default. After a device running V200R020C10 or an earlier version is upgraded to V200R020C10 or a later version, to ensure compatibility, the **undo authentication ip-address in-accounting-start** command is automatically generated in the configuration file of a switch.

Example

Enable the function of carrying users' IP addresses in Accounting-Start packets.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication ip-address in-accounting-start
```

13.5.34 authentication ipv4-address in-accounting-start mandatory

Function

The **authentication ipv4-address in-accounting-start mandatory** command enables the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets.

The **undo authentication ipv4-address in-accounting-start mandatory** command disables the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets.

By default, the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets is enabled.

Format

authentication ipv4-address in-accounting-start mandatory

undo authentication ipv4-address in-accounting-start mandatory

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

After you run the **authentication ipv4-address in-accounting-start** command to enable the function of carrying users' IP addresses in Accounting-Start packets, you can run the **authentication ipv4-address in-accounting-start mandatory** command to configure the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets. The following table lists the effectiveness of the two functions.

authentication ip-address in-accounting-start	authentication ipv4-address in-accounting-start mandatory	Effectiveness
Enabled	Enabled	The device sends an Accounting-Start packet only when a user has an IPv4 address.
Enabled	Disabled	The device sends an Accounting-Start packet only when a user has an IPv4 or IPv6 address.
Disabled	Enabled or disabled	The device can send an Accounting-Start packet regardless of whether a user has an IPv4 or IPv6 address.

Example

Enable the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication ipv4-address in-accounting-start mandatory
```

13.5.35 authentication ip-conflict-check enable

Function

The **authentication ip-conflict-check enable** command enables the client IP address conflict detection function.

The **undo authentication ip-conflict-check enable** command disables the client IP address conflict detection function.

By default, the device detects whether client IP addresses conflict with each other.

Format

authentication ip-conflict-check enable

undo authentication ip-conflict-check enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP address conflict detection is performed based on an IP hash table. If the hash value of a client IP address conflicts with a value in the IP hash table on the device, the client cannot be authenticated. To prevent unauthorized users from accessing the network using forged IP addresses, you can enable the IP address conflict detection function. Some clients may use the same fixed source IP address to send ARP probe packets. If multiple such clients exist on the network, an IP address conflict occurs. In this case, you can disable the IP address conflict detection function.

Precautions

The **undo authentication ip-conflict-check enable** command is mutually exclusive with and takes precedence over the following configurations:

- Portal authentication
- Pushed URL configured using the **force-push** command
- Redirect URL configured using the **dot1x url** command for 802.1X authentication

After IP address conflict detection is disabled:

- After users with the same IPv4 address but different MAC addresses go online, the IPv4 address is displayed only for the first online user in the user table on the device. The second user displays a conflicting IP address.
- After users with the same IPv6 address but different MAC addresses go online, the IPv6 address is displayed for each user in the user table on the device. The second user displays a conflicting IP address

Example

Enable the client IP address conflict detection function.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication ip-conflict-check enable
```

13.5.36 authentication ipv6-control enable

Function

The **authentication ipv6-control enable** command enables network admission control for IPv6 users.

The **undo authentication ipv6-control enable** command disables network admission control for IPv6 users.

By default, the network admission control function is disabled for IPv6 users.

NOTE

On the S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI that functions as the parent in an SVF system, the configuration of this command does not take effect and is delivered to ASs.

The following models do not support this command: S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S500, S5735-S-I

Format

authentication ipv6-control enable

undo authentication ipv6-control enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, after NAC authentication is enabled on the device, IPv6 users can access the network without being authenticated in some scenarios. To ensure security, access right control can be enabled for IPv6 users, so that IPv6 users can access the network after being authenticated.

Precautions

The following table lists how different products process IPv6 packets for users in different authentication states.

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/ Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI	802.1X authentication on Layer 2 Ethernet interfaces	Not permitted	Not permitted	Permitted	This command does not take effect.		
	MAC address authentication on VLANIF interfaces	Not permitted	Not permitted	Permitted			
	MAC address authentication on Layer 2 Ethernet interfaces	Not permitted	Not permitted	Permitted			
	Layer 2 Portal authentication on VLANIF interfaces	Not permitted	Not permitted	Permitted			
	Layer 2 Portal authentication on Layer 2 Ethernet interfaces	Not permitted	Not permitted	Permitted			

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/ Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
	Layer 3 Portal authentication on VLANIF interfaces	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Not permitted			
	Layer 3 Portal authentication on Layer 3 Ethernet interfaces	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Not permitted			
S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S	802.1X authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	MAC address authentication on VLANIF interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/ Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
	MAC address authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 2 Portal authentication on VLANIF interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 2 Portal authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 3 Portal authentication on VLANIF interfaces	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/ Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
	Layer 3 Portal authentication on Layer 3 Ethernet interfaces	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted
All products excluding S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S5731-L, S5731S-L	802.1X authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	MAC address authentication on VLANIF interfaces	Permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	MAC address authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 2 Portal authentication on VLANIF interfaces	Permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/ Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
	Layer 2 Portal authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 3 Portal authentication on VLANIF interfaces	Permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Not permitted
	Layer 3 Portal authentication on Layer 3 Ethernet interfaces **NOTE** This authentication mode is supported only on the S6720-EI, S6735-S, S6720S-EI.	Permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Not permitted

For Portal users who access the network through devices that support this command: When network permission control for IPv6 users is disabled and Portal

authentication redirection is enabled, CPU-bound IPv6 HTTP packets are still redirected.

Example

Enable network admission control for IPv6 users.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication ipv6-control enable
```

13.5.37 authentication mode

Function

The **authentication mode** command configures the user access mode.

The **undo authentication mode** command restores the default user access mode.

By default, the user access mode is **multi-authen**.

Format

authentication mode { **single-terminal** | **single-voice-with-data** | **multi-share** | **multi-authen** [**max-user** *max-user-number* [**dot1x** | **mac-authen** | **portal** | **none**] *] }

undo authentication mode [**multi-authen max-user** [**dot1x** | **mac-authen** | **portal** | **none**] *]

Parameters

Parameter	Description	Value
single-terminal	Configures an interface to allow only one user to go online.	-
single-voice-with-data	Configures an interface to allow only one data user and one voice user to go online. This mode applies when a data user connects to a network through a voice terminal.	-
multi-share	Configures an interface to allow multiple users to go online. In this mode, the device authenticates only the first access user. If the first user passes authentication, subsequent users share the same network access rights with the first user. If the first user goes offline, other users also go offline.	-

Parameter	Description	Value
multi-authen	Configures an interface to allow multiple users to go online. In this mode, the device authenticates each access user. If users pass authentication, the users are given individual network access rights. If a user goes offline, other users will not be affected.	-
max-user *max-user-number*	Specifies the maximum number of access users on the interface in **multi-authen** mode.	The value is an integer and the value range varies depending on devices.
dot1x	Specifies the maximum number of 802.1X authenticated users allowed to connect to the interface in **multi-authen** mode.	-
mac-authen	Specifies the maximum number of MAC authenticated users allowed to connect to the interface in **multi-authen** mode.	-
portal	Specifies the maximum number of Portal authenticated users allowed to connect to the interface in **multi-authen** mode.	-
none	Specifies the maximum number of pre-connection users allowed to connect to the interface in **multi-authen** mode.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After NAC authentication is enabled, you can configure the user access mode on an interface based on the user access on the interface.

- **single-terminal**: applies when only one data terminal is connected to the network through the interface.

- **single-voice-with-data**: applies when only one data terminal is connected to the network on the interface through a voice terminal.
- **multi-share**: applies when multiple data terminals are connected to the network on the interface and high security is not required.
- **multi-authen**: applies when multiple data terminals are connected to the network on the interface and high security is required. In this access mode, you can configure the maximum number of access users based on the actual user quantity on the interface. This prevents malicious users from occupying a large amount of device resources and ensures that the users on other interfaces can normally go online.

Precautions

- VLANIF interfaces do not support this function.
- If there are online users in the authentication profile, the user access mode cannot be changed.
- This function takes effect only for wired users.
- If the **multi-share** mode is configured on an Eth-Trunk of the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the upstream rate limit cannot be delivered to users who go online through this Eth-Trunk.
- If the first access user fails authentication on a physical interface and sets up a pre-connection after the **multi-share** mode is configured on the physical interface, new access users will also fail authentication on the interface. Therefore, the following operations are recommended if the first access user may fail authentication after the **multi-share** mode is configured on a physical interface.
  - Disable the pre-connection function using the **undo authentication pre-authen-access enable** when 802.1X or MAC authentication is used.
  - Do not use the **multi-share** mode with Portal authentication.
- In policy association scenarios, the **authentication mode multi-authen max-user** *max-user-number* command configured on an AS does not take effect. To set the maximum number of access users on an AS, run the **authentication access-point max-user** *max-user-number* command to set the maximum number of access users allowed on the interface of the access device.
- When **authentication mode** is set to **multi-authen** in the authentication profile, to configure authorized VLANs, set the interface type to hybrid or trunk in policy association scenarios, and to hybrid in other scenarios.
- When the user access mode is set to **multi-share** on the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, the following situation may occur before MAC address learning is triggered by user packets: The **display access-user** command output contains user entries but the **display mac-address** command output does not contain user MAC address entries. The **display mac-address** command displays MAC address entries only after MAC address learning is triggered by user packets.
- If the user access mode is **multi-share**, authorization redirection ACLs or authorized voice VLANs are not supported.
- If the user access mode is set to **multi-share**, authorization based on an ISP VLAN is not supported.

- If the user access mode is set to **multi-share**, authorization based on the HW-Forwarding-Interface attribute is not supported.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, if the authentication profile in which the user access mode is set to **multi-share** is applied to a physical interface and the **statistic enable** or **accounting dual-stack separate** command is configured on the interface, IPv4 and IPv6 traffic statistics are not differentiated and both counted as IPv4 traffic statistics displayed using the **display access-user** command.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500. S5735-S-I, S5735S-S, , if the authentication profile in which the user access mode is set to **multi-authen** is applied and both the **car** and **statistic enable** commands are configured, only the **car** command takes effect.

Example

In the authentication profile **p1**, set the user access mode to **multi-authen**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication mode multi-authen
```

13.5.38 authentication mac-authen-first force

Function

The **authentication mac-authen-first force** command configures forcible MAC address authentication before 802.1X authentication.

The **undo authentication mac-authen-first force** command restores the default setting.

By default, the forcible MAC address authentication is not configured before 802.1X authentication.

Format

authentication mac-authen-first force

undo authentication mac-authen-first force

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command.

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If high security is required, users who access the network must use registered terminals for 802.1X authentication. To prevent users from using unregistered terminals to perform 802.1X authentication and occupying device and server resources, you can configure this function to force the users to perform MAC address authentication first. 802.1X authentication can be performed only after MAC address authentication succeeds. For an unregistered terminal, users go offline directly after MAC address authentication fails, and 802.1X authentication is not performed.

Precautions

This function is only supported in the wireless scenario.

This command takes effect only when an 802.1X access profile and a MAC access profile have been configured in the authentication profile where the command is configured.

Example

Configure forcible MAC address authentication before 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication mac-authen-first force
```

13.5.39 authentication mac-move enable

Function

The **authentication mac-move enable** command enables MAC address migration.

The **undo authentication mac-move enable** command disables MAC address migration.

By default, MAC address migration is disabled.

Format

authentication mac-move enable vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1–10> }

undo authentication mac-move enable vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1–10> }

Parameters

Parameter	Description	Value
vlan	Specifies the VLAN range for enabling MAC address migration.	-
all	Enables MAC address migration in all VLANs.	-
vlan-id1 [**to** *vlan-id2*]	Enables MAC address migration in the specified VLANs. • *vlan-id1* specifies the start VLAN ID. • *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and *vlan-id2* define a range together. • If the parameter **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is created.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a user is authenticated and accesses the network from one interface of the device, the Ethernet cable is pulled out from the interface and plugged in another interface on the device; or a user switches between different VLANs on the same interface. In this case, the user cannot immediately initiate authentication and access the network. The user can initiate authentication on the current interface only after the user offline detection interval expires or the authentication interface is manually enabled and shut down to clear user online entries. To improve user experience, MAC address migration is enabled so that the user can immediately initiate authentication and access the network after be switched to another access interface.

MAC address migration allows online NAC authentication users to immediately initiate authentication and access the network after they are switched to other access interfaces. If the user is authenticated successfully on the new interface, the online user entry on the original interface is deleted immediately to ensure that only one interface records the online user entry.

In addition, VLANs need to be specified for users in MAC address migration. The VLANs before and after the migration can be specified for the users, and they can be the same or different.

Precautions

- In normal case, enabling MAC address migration is not recommended. It should be enabled only when users have migration requirements during roaming. This prevents unauthorized users from forging MAC addresses of online users and sending ARP, 802.1X, or DHCP packets on other authentication control interfaces to trigger the MAC address migration function and force authorized user offline.
- In the Policy Association and SVF scenario, the device does not support MAC address migration.
- In the Layer 2 BNG scenario, the device does not support MAC address migration.
- Cascading migration through intermediate devices is not supported, because ARP and DHCP packets are not sent after the cascading migration.
- The device does not support MAC address migration for a terminal with one MAC address and multiple IP addresses.
- MAC address migration is not supported for Layer 3 Portal authentication users.
- A user is switched from an interface configured with NAC authentication to another interface not configured with NAC authentication. In this case, the user can access the network only after the original online entry is aged because the new interface cannot send authentication packets to trigger MAC migration.
- In common mode, Portal authentication is triggered only after users who go online through a VLANIF interface send ARP packets and go offline; otherwise, the users can go online again only after the original user online entries age out. Portal authentication cannot be triggered after users who go online through physical interfaces migrate. The users can go online again only after the original user online entries age out.
- After a user who goes online from a VLANIF interface is quieted because of multiple MAC address migrations, MAC address migration can be performed for the quieted user only after the quiet period expires and the ARP entry is aged out.
- When an authorized VLAN is specified in the **authentication mac-move enable vlan** command, you are advised to enable the function of detecting the user status before user MAC address migration.
- When a device functions as a third-party AC for wireless-to-wire authentication and a native AC, MAC address migration is not supported when the terminal switches from the third-party Wi-Fi to the native AC Wi-Fi. The terminal can go online only after the wired authentication entry ages 5 minutes. In this scenario, you are advised to move the authentication point to a third-party AC and do not deploy wireless-to-wire authentication.

Example

Enable MAC address migration in all VLANs.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move enable vlan all
```

13.5.40 authentication mac-move detect enable

Function

The **authentication mac-move detect enable** command enables a device to detect users' online status before user MAC address migration.

The **undo authentication mac-move detect enable** command disables a device from detecting users' online status before user MAC address migration.

By default, a device is disabled from detecting users' online status before user MAC address migration.

Format

authentication mac-move detect enable

undo authentication mac-move detect enable

Parameters

None

Views

System view, authentication profile view

Default Level

2: Configuration level

Usage Guidelines

To prevent unauthorized users from spoofing online users to attack a device, run the **authentication mac-move detect enable** command to enable the device to detect users' online status before user MAC address migration. If no users are online, the device permits MAC address migration and allows users to go online from a new access interface. If a user is online, the device terminates MAC address migration and does not allow the user to go online from a new access interface.

You can also run the **authentication mac-move detect retry-interval retry-time** command to set the detection interval and maximum number of detections before user MAC address migration.

By default, the user status detection function before user MAC address migration is disabled in the system view, but it is enabled in the authentication profile view. This function takes effect only when it is enabled both in the system view and authentication profile view. To disable the device from detecting the online status

of users connected to certain interfaces before user MAC address migration, run the **undo authentication mac-move detect enable** command in the authentication profiles bound to these interfaces.

After the **authentication mac-move detect enable** command is configured in an authentication profile, the authentication profile cannot be bound to a VAP profile.

Example

Enable a device to detect users' online status before user MAC address migration.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move detect enable
```

13.5.41 authentication mac-move detect retry-interval retry-time

Function

The **authentication mac-move detect retry-interval retry-time** command sets the detection interval and maximum number of detections before user MAC address migration.

The **undo authentication mac-move detect retry-interval retry-time** command restores the default setting.

By default, a device detects users' online status once. The detection interval is 3 seconds.

Format

authentication mac-move detect { **retry-interval** *interval* | **retry-time** *times* } *

undo authentication mac-move detect { **retry-interval** | **retry-time** } *

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a device detects users' online status before user MAC address migration.	The value is an integer that ranges from 1 to 5, in seconds.
times	Specifies the maximum number of detections before user MAC address migration.	The value is an integer that ranges from 1 to 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a device is enabled to detect users' online status before user MAC address migration, if no users are online, the device permits MAC address migration and allows users to go online from a new access interface. If a user is online, the device terminates MAC address migration and does not allow the user to go online from a new access interface. You can run the **authentication mac-move detect** { **retry-interval** *interval* | **retry-time** *times* } * command to modify the default detection interval and maximum number of detections.

Example

Configure a device to detect users' online status twice at an interval of 5 seconds before user MAC address migration.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move detect retry-interval 5 retry-time 2
```

13.5.42 authentication mac-move quiet-log enable

Function

The **authentication mac-move quiet-log enable** command enables the device to record logs about MAC address migration quiet.

The **undo authentication mac-move quiet-log enable** command disables the device from recording logs about MAC address migration quiet.

By default, the device is enabled to record logs about MAC address migration quiet.

Format

authentication mac-move quiet-log enable

undo authentication mac-move quiet-log enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can record logs when adding or deleting MAC address migration quiet entries. This helps the administrator to find out the cause for MAC address migration failure, and improves maintainability of the MAC address migration quiet function.

Example

Enable the device to record logs about MAC address migration quiet.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-log enable
```

13.5.43 authentication mac-move quiet-times quiet-period

Function

The **authentication mac-move quiet-times quiet-period** command configures the quiet period and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state.

The **undo authentication mac-move quiet-times quiet-period** command restores the default settings.

The default quiet period is 0 seconds and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state is 3.

Format

authentication mac-move { **quiet-times** *times* | **quiet-period** *quiet-value* } *

undo authentication mac-move { **quiet-times** | **quiet-period** } *

Parameters

Parameter	Description	Value
times	Specifies the maximum number of MAC address migration times within 60 seconds before users enter the quiet state.	The value is an integer that ranges from 1 to 10.

Parameter	Description	Value
quiet-value	Specifies the quiet period for MAC address migration users.	The value is an integer that ranges from 0 to 3600. The value 0 indicates that the MAC address migration quiet function is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When users frequently switch access interfaces (especially frequent switching due to loops), the device needs to process a large number of authentication packets and entries, which results in high CPU usage. To solve this problem, configure the MAC address migration quiet function.

If the number of MAC address migration times for a user within 60 seconds exceeds the value (*times*) after the MAC address migration quiet function is enabled, the device quiets the user for a certain period (*quiet-value*). During the quiet period, the device does not allow users to perform MAC address migration.

Example

Configure the quiet period to 120 seconds and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state to 5.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-times 5 quiet-period 120
```

13.5.44 authentication mac-move quiet-user-alarm enable

Function

The **authentication mac-move quiet-user-alarm enable** command enables the device to send alarms about MAC address migration quiet.

The **undo authentication mac-move quiet-user-alarm enable** command disables the device from sending alarms about MAC address migration quiet.

By default, the device is disabled from sending alarms about MAC address migration quiet.

Format

authentication mac-move quiet-user-alarm enable

undo authentication mac-move quiet-user-alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can send alarms about MAC address migration quiet to improve maintainability of the MAC address migration quiet function. The device sends alarms when the percentage of the actual user amount in the MAC address migration quiet table against the maximum number of users exceeds the upper alarm threshold configured. If the percentage decreases to be equal to or smaller than the lower alarm threshold, the device sends a clear alarm. The upper and lower alarm thresholds are configured using the **authentication mac-move quiet-user-alarm percentage** command.

Example

Enable the device to send alarms about MAC address migration quiet.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-user-alarm enable
```

13.5.45 authentication mac-move quiet-user-alarm percentage

Function

The **authentication mac-move quiet-user-alarm percentage** command configures the upper and lower alarm thresholds for the percentage of MAC address migration users in quiet state.

The **undo authentication mac-move quiet-user-alarm percentage** command restores the default setting.

By default, the lower alarm threshold is 50 and upper alarm threshold is 100.

Format

authentication mac-move quiet-user-alarm percentage *lower-threshold upper-threshold*

undo authentication mac-move quiet-user-alarm percentage

Parameters

Parameter	Description	Value
lower-threshold	Specifies the lower alarm threshold.	The value is an integer that ranges from 1 to 100.
upper-threshold	Specifies the upper alarm threshold.	The value is an integer that ranges from 1 to 100. The value must be greater than that of *lower-threshold*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **authentication mac-move quiet-user-alarm enable** command can be run to enable the device to send alarms about MAC address migration quiet to improve maintainability of the MAC address migration quiet function. The device sends alarms when the percentage of the actual user amount in the MAC address migration quiet table against the maximum number of users exceeds the upper alarm threshold configured. If the percentage decreases to be equal to or smaller than the lower alarm threshold, the device sends a clear alarm. The upper and lower alarm thresholds are configured using the **authentication mac-move quiet-user-alarm percentage** command.

Precautions

When a user goes online at a rate exceeding the upper limit, the alarm may not be generated.

Example

Configure the upper alarm threshold to 80 and lower alarm threshold to 40.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-user-alarm percentage 40 80
```


13.5.46 authentication no-ip-check

Function

The **authentication no-ip-check** command disables the device from creating an IP hash table for client IP addresses.

The **undo authentication no-ip-check** command allows the device to create an IP hash table for client IP addresses.

By default, the device creates an IP hash table for client IP addresses.

Format

authentication no-ip-check

undo authentication no-ip-check

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After users obtain IP addresses, the device creates an IP hash table. If the hash value of a client IP address conflicts with a value in the IP hash table on the device, the client cannot be authenticated. When two branches are connected to the device, the address pools of the branches may overlap. As a result, two clients in different branches may have the same IP address. When the device detects conflicting IP addresses, the clients fail to go online. To address this problem, you can run the **authentication no-ip-check** command to disable the device from creating an IP hash table for client IP addresses.

Precautions

You are advised not to configure the **authentication no-ip-check** command. If this command is configured and two clients with the same IP address go online through the same interface, the rules (such as ACL rules and static UCL groups) configured based on this IP address may be mismatched.

This function cannot be used with Portal authentication together.

This function cannot be configured with **ip-static-user enable** together.

After this function is enabled, network access permissions are granted only to users in the ARP table.

After the **authentication no-ip-check** command is run, IP address–based CoA cannot be implemented.

Example

Disable the device from creating an IP hash table for client IP addresses.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication no-ip-check
```

13.5.47 authentication no-replace dot1x

Function

The **authentication no-replace dot1x** command configures the device not to respond to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

The **undo authentication no-replace dot1x** command configures the device to respond to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

By default, the device responds to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

Format

authentication no-replace dot1x [**device-type voice**]

undo authentication no-replace dot1x [**device-type voice**]

Parameters

Parameter	Description	Value
device-type voice	Configures the function to be effective only for voice terminals. When this parameter is not specified, the function is effective for all terminals.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After passing MAC address authentication, some voice terminals still send EAP start packets. If the device returns response packets, the voice terminals go offline. To address this problem, you can configure the device not to respond to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

Precautions

This function is effective only for wired users.

No matter whether this function is configured, the device responds to EAP Start packets sent from 802.1X users.

Example

Configure the device not to respond to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication no-replace dot1x device-type voice
```

13.5.48 authentication order mac dot1x

Function

The **authentication order mac dot1x** command configures MAC address authentication to take precedence over 802.1X authentication when the device receives EAP-Start packets.

The **undo authentication order mac dot1x** command cancels the configuration.

By default, the sequence of authentication modes triggered by EAP-Start packets is not configured.

Format

authentication order mac dot1x

undo authentication order mac dot1x

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some terminals send EAP-Start packets to trigger 802.1X authentication, but do not respond to EAP-Request/Identity packets returned by the device. As a result, traffic is interrupted and the terminals cannot be authenticated. To authenticate these terminals, you can run the **authentication order mac dot1x** command to enable the device to perform MAC address authentication first after receiving EAP-Start packets. If the terminals fail the MAC address authentication, the device then performs 802.1X authentication.

If a terminal sends multiple EAP-Start packets, the device continues to return EAP-Response/Identity packets even after MAC address authentication using the first EAP-Start packet is successful. However, the terminal no longer responds to the subsequent EAP-Response/Identity packets, causing traffic interruption. To prevent this problem, run the **authentication no-replace dot1x** command to configure the device not to respond to the EAP-Start packets sent from users who have successfully passed MAC address authentication.

Precautions

This function is supported only for new wired users.

This command controls only the sequence of authentication modes triggered by EAP-Start packets. After this command is run, MAC address authentication or 802.1X authentication will not be automatically enabled.

This command takes precedence over the **authentication dot1x-mac-bypass** command.

Example

Configure MAC address authentication to take precedence over 802.1X authentication when the device receives EAP-Start packets.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication order mac dot1x
```

13.5.49 authentication pre-authen-access enable

Function

The **authentication pre-authen-access enable** command enables the pre-connection function.

The **undo authentication pre-authen-access enable** command disables the pre-connection function.

By default, the pre-connection function is enabled. That is, the device keeps users who are not successfully authenticated and do not have any network access permissions in the pre-connection state.

Format

authentication pre-authen-access enable

undo authentication pre-authen-access enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user terminal connects to an NAC-enabled interface on the device, a pre-connection is set up between the terminal and device. If the device is not configured to grant network access rights to users in pre-connection or authentication failure state, users who fail to be authenticated remain in the pre-connection state by default. Because the device allows DHCP packets from pre-connection users to pass through, the users can still obtain IP addresses although they do not have any network access rights, wasting IP addresses and bringing network security risks.

If users do not need any network access rights before being authenticated successfully, disable the pre-connection function. Users will then not have any network access rights before being authenticated successfully and will not obtain IP addresses.

Precautions

- This function does not take effect for users who use Portal authentication or combined authentication (including Portal authentication).
- The **undo authentication pre-authen-access enable** command does not take effect for pre-connection users for whom network access permissions are configured.
- When the **lldp sensor-ap authentication disable** command is configured in the authentication profile view, the **undo authentication pre-authen-access enable** command does not take effect.
- When 802.1X authentication or MAC address authentication is configured on a physical interface, the **free-rule** command configuration will not take effect after the pre-connection function is disabled.
- If the device connects to some terminals such as a MacBook laptop that is not authenticated after obtaining an IP address, it is recommended that you run the **undo authentication pre-authen-access enable** command on the device to disable the pre-connection function and then connect the terminal to the network again.
- If a user in pre-connection state attempts to go online using DHCP packets containing the Option 82 field but fails to go online, it is recommended that

you run the **undo authentication pre-authen-access enable** command on the device to disable the pre-connection function.

- When Layer 2 Portal authentication is deployed on a non-gateway device, do not run the **undo authentication pre-authen-access enable** command to disable the pre-connection function. Otherwise, Layer 2 Portal authentication will not take effect.
- When MAC address authentication or Portal authentication is configured on a physical interface, no pre-connection entry is generated, but users can go online successfully.

Example

Disable the pre-connection function.

```
<HUAWEI> system-view
[HUAWEI] undo authentication pre-authen-access enable
```

13.5.50 authentication port-vlan-modify user-online

Function

The **authentication port-vlan-modify user-online** command enables the function of keeping users online when the port type or VLAN is changed.

The **undo authentication port-vlan-modify user-online** command restores the default setting.

By default, the function of keeping users online when the port type or VLAN is changed is disabled.

Format

authentication port-vlan-modify user-online

undo authentication port-vlan-modify user-online

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After user access authentication succeeds, you can change the VLAN allowed to access or the access interface type through the RADIUS server. For example, you

can assign VLANs to clients through the server for network planning and deployment. After the deployment is complete, to reduce the impact of link faults and device restart on the network and implement rapid network restoration, you can change the user access VLAN to the authorized VLAN. In this case, you can enable the function of keeping users online when the port type or VLAN is changed to modify interface or VLAN configurations.

Precautions

This function is only supported by MAC and 802.1X authentication.

This function is only supported by wired users.

Example

Enable the function of keeping users online when the port type or VLAN is changed.

```
<HUAWEI> system-view
[HUAWEI] authentication port-vlan-modify user-online
```

13.5.51 authentication { roam-accounting | update-info-accounting | update-ip-accounting } * enable

Function

The **authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command enables a device to send accounting packets for roaming, terminal information updating and address updating.

The **undo authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command disables a device from sending accounting packets for roaming, terminal information updating and address updating.

By default, the device is enabled to send accounting packets for roaming, terminal information updating and address updating.

Format

authentication { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable**

undo authentication { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable**

NOTE

Only the following models support **roam-accounting**:
S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

By default, the device sends accounting packets for roaming, terminal information, and address updating to the accounting server. Some accounting servers may not require the accounting packets. In this case, resources on the device are occupied. You can run the **undo authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command to disable a device from sending accounting packets for roaming, terminal information updating and address updating, saving resources on the device. After roaming, terminal information updating, and address updating are complete, the device sends accounting packets again and the accounting function is not affected.

In the command:

- **roam-accounting** indicates that accounting packets are immediately sent during roaming.
- Only wireless user devices support the **roam-accounting** parameter.
- **update-info-accounting** indicates that accounting packets are immediately sent during terminal information updating.

  To configure this function, the terminal type identification function must be configured simultaneously.
- **update-ip-accounting** indicates that accounting packets are immediately sent during address updating.
- If the terminal information (including the DHCP Option, user agent, or LLDP information) is updated for the first time, the device immediately triggers real-time accounting. If the terminal information is not updated for the first time, the device only updates the user entry and reports the new terminal information through subsequent accounting messages.
- After the **undo authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command is configured, the device does not send the accounting packet immediately after obtaining the packet, and waits until the real-time accounting timer expires.

Example

Disable a device from sending accounting packets for address updating.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] undo authentication update-ip-accounting enable
```


13.5.52 authentication roam pre-authen mac-authen enable

Function

The **authentication roam pre-authen mac-authen enable** command enables MAC address authentication for roaming STAs.

The **undo authentication roam pre-authen mac-authen enable** command disables MAC address authentication for roaming STAs.

By default, MAC address authentication is disabled for roaming STAs.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command.

Format

authentication roam pre-authen mac-authen enable

undo authentication roam pre-authen mac-authen enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A STA connects to the network through MAC address authentication or MAC address-prioritized Portal authentication. If the STA roams, MAC address authentication is triggered after successful roaming. However, MAC address authentication may fail, and the STA enters the pre-connection state and no longer has the original access permission. To prevent this problem, the MAC address authentication is disabled for roaming STAs by default. You are not advised to retain the default configuration.

Precautions

MAC address authentication for roaming STAs takes effect only when the following authentication event authorization information is configured:

- Authorization for STAs in pre-connection users
- Authorization for STAs that fail the authentication
- Authorization for STAs if the authorization server goes Down

- Authorization for STAs if the Portal server goes Down

Example

Enable MAC address authentication for roaming STAs.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication roam pre-authen mac-authen enable
```

13.5.53 authentication redirect-acl original-url enable

Function

The **authentication redirect-acl original-url enable** command configures the redirect URL to carry the original URL when Portal-authenticated users who match a redirect ACL are forcibly redirected for another forcible Portal authentication.

The **undo authentication redirect-acl original-url enable** command restores the default configuration.

By default, the redirect URL does not carry the original URL.

Format

authentication redirect-acl original-url enable

undo authentication redirect-acl original-url enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An administrator may need to redirect the Portal-authenticated users who match a redirect ACL to a specified web page for another forcible Portal authentication. By default, the redirect URL does not carry the original URL accessed by users. After successful forcible authentication, the authentication server cannot obtain the original URL, causing the failure to access the original URL. To resolve this problem, run the **authentication redirect-acl original-url enable** command to configure the redirect URL to carry the original URL.

Precautions

Only the users who have passed Portal authentication and match a redirect ACL can be redirected to a specified web page for another forcible Portal authentication.

Before the function takes effect, you must run the **url-parameter** command in the Portal server template view to configure the original URL parameter to be carried in the redirect URL.

Example

Configure the redirect URL to carry the original URL.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication redirect-acl original-url enable
```

13.5.54 authentication single-access

Function

The **authentication single-access** command configures the device to allow users to access in only one authentication mode.

The **undo authentication single-access** command restores the default setting.

By default, the device allows users to access in different authentication modes.

Format

authentication single-access

undo authentication single-access

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

After hybrid authentication is configured, the device by default allows users to access in different authentication modes. You can run the **authentication single-access** command to disable this default function. The device then allows users to access in only one authentication mode and does not process the packets of other authentication modes.

Example

In the authentication profile **authen1**, configure the device to allow users to access in only one authentication mode.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication single-access
```

13.5.55 authentication single-stack-control enable

Function

The **authentication single-stack-control enable** command enables the single-stack authentication function.

The **undo authentication single-stack-control enable** command disables the single-stack authentication function.

By default, the single-stack authentication function is disabled.

NOTE

This command takes effect only on the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

This command does not take effect on other switch models. However, it can be run to deliver configurations to ASs when the device functions as an SVF parent.

Format

authentication single-stack-control { **ipv4** | **ipv6** } **enable**

undo authentication single-stack-control enable

Parameters

Parameter	Description	Value
ipv4	Enables the single-stack authentication function for IPv4 traffic.	-
ipv6	Enables the single-stack authentication function for IPv6 traffic.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, access control is not performed for IPv4 or IPv6 traffic. You can use this command to configure single-stack authentication to control IPv4 or IPv6 traffic separately.

Precautions

This function takes effect only on wired Portal users.

Example

Enable single-stack authentication for IPv6 traffic in the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication single-stack-control ipv6 enable
```

13.5.56 authentication speed-limit auto

Function

The **authentication speed-limit auto** command enables the device to dynamically adjust the rate of packets from NAC users.

The **undo authentication speed-limit auto** command disables the device from dynamically adjusting the rate of packets from NAC users.

By default, the device does not dynamically adjust the rate of packets from NAC users.

Format

authentication speed-limit auto

undo authentication speed-limit auto

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a lot of NAC users send authentication or log off requests to the device, the CPU usage may be overloaded especially when the CPU or memory usage is

already high (for example, above 80%). After the device is enabled to dynamically adjust the rate of packets from NAC users, the device limits the number of NAC packets received per second if the CPU or memory usage is high. This function reduces loads on the device CPU.

Example

Enable the device to dynamically adjust the rate of packets from NAC users.

```
<HUAWEI> system-view
[HUAWEI] authentication speed-limit auto
```

13.5.57 authentication termination-action reauthenticate

Function

The **authentication termination-action reauthenticate** command configures the device to re-authenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

The **undo authentication termination-action** command restores the default setting.

By default, the device is not configured to re-authenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

Format

authentication termination-action reauthenticate

undo authentication termination-action

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RADIUS server uses the **Session-Timeout** attribute to control the remaining online time of a user, and uses the **Termination-Action** attribute to determine whether to re-authenticate the user when the timeout interval expires. By default, if the RADIUS server delivers **Session-Timeout** but no **Termination-Action**, the device disconnects users when the time exceeds the value of **Session-Timeout**. To re-authenticate users without modifying the server configuration, you can run this

command to configure the device to re-authenticate users when the timeout interval expires.

Precautions

Only 802.1X authentication and MAC address authentication on Layer 2 interfaces support this function.

Example

In authentication profile **authen1**, configure the device to re-authenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication termination-action reauthenticate
```

13.5.58 authentication timer handshake-period

Function

The **authentication timer handshake-period** command sets the handshake interval of the device with pre-connection users and authorized users.

The **undo authentication timer handshake-period** command restores the default setting.

The default handshake interval of the device with pre-connection users and authorized users is 300 seconds.

Format

authentication timer handshake-period *handshake-period*

undo authentication timer handshake-period

Parameters

Parameter	Description	Value
handshake-period	Specifies the handshake interval.	The value is an integer in the range from 5 to 7200, in seconds.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the handshake with pre-connection users and authorized users using the **authentication handshake** command, you can run the **authentication timer handshake-period** command to set the handshake interval. After that, if a user does not respond to the handshake request from the device within the handshake interval, the device deletes the user entry.

Precautions

- This command applies only to MAC address authentication, Layer 3 Portal authentication and 802.1X authentication.
- For Layer 3 Portal authentication users, only those who go online through S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this function.
- This function takes effect only for the wired users. For wired users who do not obtain IP addresses within 30 minutes, traffic detection will be performed (detection process can be seen as the following precautions). If traffic passes through the device, users are online. If no traffic passes through the device, users go offline.
- This function takes effect only for users who go online after this function is successfully configured.
- The handshake function is implemented using ARP probe packets or neighbor discovery (ND) probe packets.
- The handshake function can also be implemented by detecting whether there is user traffic on the access device. Assuming that the handshake interval is **3n**, the device will detect user traffic at **n** and **2n**. The following uses the **0-n** period as an example. The process during the **n-2n** period is similar to that during **0-n**. (This process applies only to authentication users who go online from the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI. Other switch models do not detect user traffic and send probe packets at **n** and **2n**.)
  - If user traffic passes the device during the **0-n** period, the device considers that the user is online at **n**, so it will not send a probe packet to the user, but resets the handshake interval.
  - If no user traffic passes the device during the **0-n** period, the device cannot determine whether the user is online at **n**, so it sends a probe packet to the user. If the device receives the reply packet from the user, it considers the user online and resets the handshake interval. If no reply packet is received, it considers the user offline.
  - If user traffic passes the device during the **2n-3n** period, the device considers that the user is online at **3n** and resets the handshake interval.
  - If no user traffic passes the device during the **2n-3n** period, the device cannot determine whether the user is online at **3n** and considers that the user is offline.

  If the device considers that the user is offline at **n**, **2n**, and **3n**, the device deletes all entries related to the user. To prevent the user from going offline unexpectedly when no operation is performed on the PC, do not set a short handshake period.

- For the models that do not support the handshake function implemented by detecting whether there is user traffic on the access device, if the number of ARP probe packets exceeds the default CAR value, the probe fails and the users are logged out (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.). To resolve the problem, the following methods are recommended:
  - Increase the handshake interval based on the number of users. The default handshake interval is recommended when there are less than 8000 users; the handshake interval should be no less than 600 seconds when there are more than 8000 users.
  - Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

Example

In the authentication profile **p1**, set the handshake interval of the device with pre-connection users and authorized users to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication timer handshake-period 200
```

13.5.59 authentication timer authen-fail-aging

Function

The **authentication timer authen-fail-aging** command configures the aging time for entries of the users who fail to be authenticated.

The **undo authentication timer authen-fail-aging** command restores the default aging time for entries of the users who fail to be authenticated.

By default, the aging time for entries of the users who fail to be authenticated is 23 hours.

Format

authentication timer authen-fail-aging *aging-time*

undo authentication timer authen-fail-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After network access policies are configured for users who fail to be authenticated, the device creates entries for these users. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.

The entries of the users who fail to be authenticated share device resources with the entries of the users who are authenticated. If there are excess entries of the users who fail to be authenticated, other users fail to be authenticated. To solve this problem, run the **authentication timer authen-fail-aging** command to reduce the aging time for entries of the users who fail to be authenticated. In addition, if the time that the users who fail to be authenticated have network access policies should be shortened, you can run this command to decrease the aging time for the user entries.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Only wired users support this function.

This function controls the aging time of user entries in the **Client-no-resp**, **Aaa-server-down** or **web-server-down** state.

Example

In the authentication profile **p1**, configure the aging time for entries of the users who fail to be authenticated to 3600 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication timer authen-fail-aging 3600
```

13.5.60 authentication timer authorize-keep-aging

Function

The **authentication timer authorize-keep-aging** command configures the aging time for entries of online users who retain original network access rights.

The **undo authentication timer authorize-keep-aging** command restores the default setting.

By default, the aging time for entries of online users who retain the original network access rights is 0. That is, these entries are not aged out by default.

Format

authentication timer authorize-keep-aging *aging-time*

undo authentication timer authorize-keep-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **authentication event action authorize keep** command is run, if the authentication server is Down or does not respond, online users retain the original network access rights. In this case, the device creates entries for the online users who retain the original network access rights. If the authentication server is always Down or does not respond, these users always retain the original network access rights. To prevent this problem, run the **authentication timer authorize-keep-aging** command to adjust the aging time of these online user entries. When the aging time expires, these online users are logged out.

Precautions

The **authentication timer authorize-keep-aging** command configuration takes effect after the **authentication event authen-server-down action close re-authen** command is executed to disable re-authentication when the authentication server is Down.

Example

Set the aging time for entries of online users who retain the original network access rights to 600s.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication timer authorize-keep-aging 600
```

13.5.61 authentication timer pre-authen-aging

Function

The **authentication timer pre-authen-aging** command configures the aging time for pre-connection user entries.

The **undo authentication timer pre-authen-aging** command restores the default aging time for pre-connection user entries.

By default, the aging time for pre-connection user entries is 23 hours.

Format

authentication timer pre-authen-aging *aging-time*

undo authentication timer pre-authen-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a pre-connection is established between the device and a user, the device creates the pre-connection user entry. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.

The pre-connection user entries share device resources with the entries of the users who are authenticated. If there are excess pre-connection user entries, other users fail to be authenticated. To solve this problem, run the **authentication timer pre-authen-aging** command to reduce the aging time for the pre-connection user entries. In addition, if the time that the pre-connection users have network access policies should be extended, you can run this command to increase the aging time for the pre-connection user entries.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Only wired users support this function.

Example

In the authentication profile **p1**, configure the aging time for the pre-connection user entries to 3600 seconds.


```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication timer pre-authen-aging 3600
```

13.5.62 authentication timer re-authen

Function

The **authentication timer re-authen** command configures the interval for re-authenticating pre-connection users or users who fail authentication.

The **undo authentication timer re-authen** command restores the default setting.

By default, for wired users, the device re-authenticates pre-connection users or users who fail authentication at an interval of 60 seconds; for wireless users, the device re-authenticates pre-connection users or users who fail authentication at an interval of 0 seconds, that is, the re-authentication function is disabled for pre-connection users or users who fail authentication; for wireless users, the device re-authenticates pre-connection users or users who fail authentication at an interval of 300 seconds.

Format

authentication timer re-authen { **pre-authen** *re-authen-time* [**wlan-user**] | **authen-fail** *re-authen-time* [**wlan-user**] }

undo authentication timer re-authen { **pre-authen** [**wlan-user**] | **authen-fail** [**wlan-user**] }

NOTE

Only S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **wlan-user** parameter.

Parameters

Parameter	Description	Value
pre-authen *re-authen-time*	Specifies the interval for re-authenticating pre-connection users.	The value can be 0 or an integer in the range from 30 to 7200, in seconds. The value 0 indicates that the re-authentication function is disabled for pre-connection users.
authen-fail *re-authen-time*	Specifies the interval for re-authenticating users who fail authentication.	The value can be 0 or an integer in the range from 30 to 7200, in seconds. The value 0 indicates that the re-authentication function is disabled for users who fail authentication.

Parameter	Description	Value
wlan-user	Indicates wireless users. If this parameter is not specified, the user type is wired users.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device creates user entries when network access rights are assigned to pre-connection users or users who fail authentication. To enable users to pass authentication in real time, the device periodically re-authenticates pre-connection users or users who fail authentication according to user entries. Administrators can adjust the re-authentication interval based on the actual network requirements.

Precautions

This command applies only to 802.1X authentication and MAC address authentication.

This function takes effect only for users who go online after this function is successfully configured.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

If a static user that has 802.1X authentication configured enters the pre-connection state after failing authentication, 802.1X authentication will be performed. During 802.1X authentication, the re-authentication interval specified by the **pre-authen** *re-authen-time* parameter does not take effect. If 802.1X authentication fails, the re-authentication interval takes effect, and re-authentication will be triggered for the static user based on this interval.

If both 802.1X authentication and MAC address authentication are configured, within the re-authentication interval specified by the **pre-authen** *re-authen-time* parameter, MAC address authentication is performed first, and 802.1X authentication is performed if MAC address authentication fails.

Example

In the authentication profile **authen1**, set the interval for re-authenticating users who fail authentication to 300 seconds.


```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication timer re-authen authen-fail 300
```

13.5.63 authentication traffic-control strict

Function

The **authentication traffic-control strict** command enables strict control on IPv4 traffic of users in pre-connection state.

The **undo authentication traffic-control strict** command restores the default configuration.

By default, strict control on IPv4 traffic of users in pre-connection state is disabled.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S support this function.

Format

authentication traffic-control strict

undo authentication traffic-control strict

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IPv4 traffic of users in pre-connection state is processed as follows:

- IPv4 unicast packets: discarded
- IPv4 multicast, broadcast, ARP, and DHCP packets: forwarded

After the **authentication traffic-control strict** command is run to enable strict control on IPv4 traffic of users in pre-connection state, IPv4 multicast, broadcast, ARP, and DHCP packets of these users are also discarded in addition to IPv4 unicast packets.

Precautions

- For details about IPv6 traffic forwarding behaviors and control, see the **authentication ipv6-control enable** command.

- In the following scenarios, the default IPv4 traffic forwarding behaviors are retained for users in pre-connection state, regardless of whether the **authentication traffic-control strict** command is configured:
  - Authentication is configured on a VLANIF interface.
  - The device functions as an AS in the policy association or SVF scenario.
  - An authentication-free rule is configured globally.
  - Portal authentication is configured in an authentication profile.
  - Authorization is configured for users in pre-connection state.

Example

Enable strict control on IPv4 traffic of users in pre-connection state.

```
<HUAWEI> system-view
[HUAWEI] authentication traffic-control strict
```

13.5.64 authentication trigger-condition (802.1X authentication)

Function

The **authentication trigger-condition** command configures the packet types that can trigger 802.1X authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP/DHCPv6/ND packets can trigger 802.1X authentication.

Format

authentication trigger-condition { **dhcp** | **arp** | **dhcpv6** | **nd** | **any-l2-packet** } *

undo authentication trigger-condition [**dhcp** | **arp** | **dhcpv6** | **nd** | **any-l2-packet**] *

Parameters

Parameter	Description	Value
dhcp	Triggers 802.1X authentication through DHCP packets.	-
arp	Triggers 802.1X authentication through ARP packets.	-
dhcpv6	Triggers 802.1X authentication through DHCPv6 packets.	-
nd	Triggers 802.1X authentication through ND packets.	-

Parameter	Description	Value
any-l2-packet	Triggers 802.1X authentication through any packets. For multicast packets, the corresponding protocol needs to be enabled, otherwise 802.1X authentication cannot be triggered. **NOTE** If only this parameter is specified in the command, DHCP, ARP, DHCPv6, and ND packets cannot trigger 802.1X authentication.	-

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After 802.1X authentication is enabled, the device can trigger 802.1X authentication on users by default when receiving DHCP, DHCPv6, ND, or ARP packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger 802.1X authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger 802.1X authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger 802.1X authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

If a static IPv4 address is configured for a client, 802.1X authentication cannot be triggered because they do not exchange DHCP, DHCPv6, ND, or ARP packets. You can run the **authentication trigger-condition any-l2-packet** command to trigger 802.1X authentication through any packets. To prevent unauthorized users from occupying user entries on the device maliciously, you are advised to configure the function of triggering 802.1X authentication through any packets on the access device, and run the **authentication mode max-user** *max-user-number* command in the authentication profile view to configure the maximum number of access users allowed on an interface. The recommended value is 10.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

To allow BPDUs to trigger 802.1X authentication, you must enable the function corresponding to the BPDUs globally. For example, to allow LLDPDUs to trigger 802.1X authentication, run the **lldp enable** command to enable LLDP globally.

When **any-l2-packet** is configured and 802.1X authentication is enabled on an interface, EAP packets sent from a client trigger 802.1X authentication first.

In a policy association scenario, 802.1X authentication can only be triggered by EAP or DHCP or ARP or DHCPv6 or ND packets.

When MAC address authentication and 802.1X authentication are both enabled on an interface, packets that can trigger authentication include all the packet types that can trigger authentication in the MAC access profile and 802.1X access profile. For example, assume that ARP packets in the MAC access profile are unable to trigger authentication and ARP packets in the 802.1X access profile can trigger authentication. If MAC address authentication and 802.1X authentication are both enabled on an interface, ARP packets can trigger MAC address authentication.

For the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the **ip-static-user enable** and **authentication trigger-condition any-l2-packet** commands are both configured, user authentication cannot be triggered by any packets.

When the pre-connection function is disabled and only 802.1X authentication is enabled on the interface, you need to use the **dot1x unicast-trigger** command to enable 802.1X authentication triggered by unicast packets so that the packet type configured in this command can trigger authentication.

Example

In the 802.1X access profile **d1**, configure the device to use DHCP packets to trigger 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] authentication trigger-condition dhcp
```

13.5.65 authentication trigger-condition (MAC address authentication)

Function

The **authentication trigger-condition** command configures the packet types that can trigger MAC address authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP/DHCPv6/ND packets can trigger MAC address authentication.

Format

authentication trigger-condition { **dhcp** | **arp** | **dhcpv6** | **nd** | **any-l2-packet** } *

undo authentication trigger-condition [**dhcp** | **arp** | **dhcpv6** | **nd** | **any-l2-packet**] *

Parameters

Parameter	Description	Value
dhcp	Triggers MAC address authentication through DHCP packets.	-
arp	Triggers MAC address authentication through ARP packets.	-
dhcpv6	Triggers MAC address authentication through DHCPv6 packets.	-
nd	Triggers MAC address authentication through ND packets.	-
any-l2-packet	Triggers MAC address authentication through any packets. For multicast packets, the corresponding protocol needs to be enabled, otherwise MAC authentication cannot be triggered. **NOTE** If only this parameter is specified in the command, DHCP, ARP, DHCPv6, and ND packets cannot trigger MAC address authentication.	-

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MAC address authentication is enabled, the device can trigger MAC address authentication on users by default when receiving DHCP/ARP/DHCPv6/ND packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger MAC address authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger MAC address authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger MAC address authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

If a static IPv4 address is configured for a client, MAC address authentication cannot be triggered because they do not exchange DHCP or ARP packets. You can run the **authentication trigger-condition any-l2-packet** command to trigger MAC address authentication through any packets. To prevent unauthorized users from occupying user entries on the device maliciously, you are advised to

configure the function of triggering MAC address authentication through any packets on the access device, and run the **authentication mode max-user** *max-user-number* command in the authentication profile view to configure the maximum number of access users allowed on an interface. The recommended value is 10.

Precautions

- MAC address authentication configured on a VLANIF interface can be triggered by ARP or ND packets if the device has learned the ARP or ND entries of user terminals.
- This function takes effect only for users who go online after this function is successfully configured.
- There is a situation that you should notice. A device is configured to trigger MAC address authentication through DHCP packets and DHCP options are used as the user names for MAC address authentication (for the configuration of user names in MAC address authentication, see **mac-authen username**). If the authentication server delivers Huawei extended RADIUS attribute HW-Forwarding-VLAN (No. 26-161) to the device, the user packet must carry double VLAN tags and the outer VLAN ID cannot be the same as the ID of HW-Forwarding-VLAN; otherwise, the delivered attribute cannot take effect.
- Only wired users support MAC address authentication triggered by DHCP/ARP/DHCPv6/ND/any packets. For wireless users, MAC address authentication is triggered by association packets.
- After the **authentication trigger-condition** { **dhcp** | **dhcpv6** | **nd** } * command is run, static users cannot go online.
- To allow BPDUs to trigger MAC address authentication, you must enable the function corresponding to the BPDUs globally. For example, to allow LLDPDUs to trigger MAC address authentication, run the **lldp enable** command to enable LLDP globally.
- In a policy association scenario, MAC address authentication can only be triggered by DHCP or ARP or DHCPv6 or ND packets.
- When MAC address authentication is performed for IP phones and the voice VLAN service is deployed, if the **authentication trigger-condition any-l2-packet** command is run to configure the device to trigger MAC address authentication through any packets, you need to run the **authentication mac-move enable** command to configure MAC address migration and run the **authentication mac-move detect enable** command to configure the device to detect users' online status before MAC address migration.
- When **any-l2-packet** is configured and 802.1X authentication is enabled on an interface, EAP packets sent from a client trigger 802.1X authentication first.
- When MAC address authentication and 802.1X authentication are both enabled on an interface, packets that can trigger authentication include all the packet types that can trigger authentication in the MAC access profile and 802.1X access profile. For example, assume that ARP packets in the MAC access profile are unable to trigger authentication and ARP packets in the 802.1X access profile can trigger authentication. If MAC address authentication and 802.1X authentication are both enabled on an interface, ARP packets can trigger MAC address authentication.

- For the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the **ip-static-user enable** and **authentication trigger-condition any-l2-packet** commands are both configured, user authentication cannot be triggered by any packets.

Example

In the MAC access profile **m1**, configure the device to trigger MAC address authentication only through ARP packets.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] authentication trigger-condition arp
```

13.5.66 authentication trigger-condition dhcp dhcp-option

Function

The **authentication trigger-condition dhcp dhcp-option** command enables the device to send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

The **undo authentication trigger-condition dhcp dhcp-option** command restores the default configuration.

By default, the device does not send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

Format

authentication trigger-condition dhcp dhcp-option *option-code*

undo authentication trigger-condition dhcp dhcp-option *option-code*

Parameters

Parameter	Description	Value
option-code	Specifies the option that the device sends to the authentication server.	The value is fixed as 82.

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Option82 records information about DHCP user locations and services (voice and data services). After this command is run, if the device can trigger MAC address authentication though DHCP packets, it sends Option82 information to the authentication server when triggering MAC address authentication through DHCP packets. Based on the user information recorded in Option82, the authentication server then assigns different network access rights to users with different services in different locations. This implements accurate control on the network access rights of each user.

Precautions

- MAC address authentication users who go online through VLANIF interfaces do not support this function.
- This function takes effect only for users who go online after this function is successfully configured.
- Only wired users support MAC address authentication triggered by DHCP/ARP/DHCPv6/ND/any packets. For wireless users, MAC address authentication is triggered by association packets.

Example

In the MAC access profile **m1**, enable the device to send Option82 information to the authentication server when triggering MAC address authentication through DHCP packets.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] authentication trigger-condition dhcp dhcp-option 82
```

13.5.67 authentication unified-mode

Function

The **authentication unified-mode** command switches the NAC mode to unified mode.

The **undo authentication unified-mode** command switches the NAC mode to common mode.

By default, the unified NAC configuration mode is used.

Format

authentication unified-mode

undo authentication unified-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with the common mode, the unified mode uses the modular configuration, making the configuration clearer and configuration model easier to understand.

Considering advantages of the unified mode, you are advised to deploy NAC in unified mode. You can run the **authentication unified-mode** command to switch the NAC mode to unified mode.

Precautions

- Starting from V200R005C00, the default NAC mode changes from common mode to unified mode. Therefore, if the system software of a switch is upgraded from a version earlier than V200R005C00 to V200R005C00 or a later version, the switch automatically runs the **undo authentication unified-mode** command to configure the NAC mode to common mode.
- After the common mode and unified mode are switched, the device automatically restarts, causing service interruption.
- In V200R008C00, some NAC commands do not differentiate the common and unified modes. Their formats and views remain unchanged after being switched from one mode to the other. After devices are switched from the common mode in V200R008C00 or later versions to the unified mode in V200R009C00 or later versions, these NAC commands can be switched to the unified mode.
- In the unified mode, only the commands of the common mode are unavailable; in the common mode, only the commands of the unified mode are unavailable. In addition, after the configuration mode is switched, the commands supported by both the common mode and unified mode still take effect.

Example

Switch the NAC mode to unified mode.

```
<HUAWEI> system-view
[HUAWEI] authentication unified-mode
```

13.5.68 authentication user-alarm percentage

Function

The **authentication user-alarm percentage** command sets alarm thresholds for the percentage of successfully authenticated NAC users.

The **undo authentication user-alarm** command restores the default alarm thresholds for the percentage of successfully authenticated NAC users.

By default, the lower alarm threshold for the percentage of successfully authenticated NAC users is 50, and the upper alarm threshold is 100.

Format

authentication user-alarm percentage *percent-lower-value percent-upper-value*

undo authentication user-alarm

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of successfully authenticated NAC users.	The value is an integer in the range from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of successfully authenticated NAC users.	The value is an integer in the range from 1 to 100, and must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the number of successfully authenticated NAC users reaches a specified percentage, the device generates an alarm. You can run the **authentication user-alarm percentage** command to set the upper and lower alarm thresholds for this percentage.

When the percentage of successfully authenticated NAC users against the maximum number of users allowed by the device is greater than or equal to the upper alarm threshold, the device generates an alarm. When this percentage reaches or falls below the lower alarm threshold, the device generates a clear alarm.

Example

Set the lower and upper alarm thresholds for the percentage of successfully authenticated NAC users to 30 and 80, respectively.

```
<HUAWEI> system-view
[HUAWEI] authentication user-alarm percentage 30 80
```


13.5.69 authentication-profile (Interface view or VAP profile view)

Function

The **authentication-profile** command applies an authentication profile to the interface or VAP profile.

The **undo authentication-profile** command restores the default setting.

By default, no authentication profile is applied to the interface or VAP profile.

Format

authentication-profile *authentication-profile-name*

undo authentication-profile

Parameters

Parameter	Description	Value
authentication-profile-name	Specifies the name of an authentication profile.	The value must be an existing authentication profile name.

Views

Interface view, or VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An authentication profile uniformly manages NAC configuration. The authentication profile is bound to the interface or VAP profile view to enable NAC, implementing access control on the users in the interface or VAP profile. The authentication type of the users in the interface or VAP profile is determined by the access profile bound to the authentication profile.

Prerequisites

An authentication profile has been created using the **authentication-profile** command in the system view.

Precautions

When configuring NAC, pay attention to the following points:

- VLANIF interfaces, Ethernet interfaces, GE interfaces, MultiGE interfaces, XGE interfaces, 25GE interface, 40GE interfaces, 100GE interfaces, Eth-Trunks, port groups, and VAP profiles support NAC. The support for NAC on different interfaces is as follows:
  - The VLANIF interface does not support 802.1X authentication.
  - Layer 2 interfaces and VLANIF interfaces support MAC address authentication. When MAC address authentication is enabled on a VLANIF interface, the IP address in the ARP packet that triggers MAC address authentication must be on the same network segment as the IP address of the VLANIF interface. (Only S5720I-SI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support configuration of MAC address authentication on VLANIF interfaces.)
  - The support for Portal authentication varies depending on different interfaces, routed main interfaces (Only S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI) support only Layer 3 Portal authentication, Layer 2 interfaces support only Layer 2 Portal authentication, and VLANIF interfaces support both Layer 2 and Layer 3 Portal authentication.
  - The VLANIF interface corresponding to the super VLAN does not support Portal authentication.
- When the user VLAN or interface type needs to be switched for an online user or a user in pre-connection state, you are advised to log out the user or shut down the interface first. Otherwise, the client may send an ARP packet to go online in VLAN 1 during the switching. As a result, the IP address of the user cannot be updated later.
- For the access of wireless users through APs, ensure that the APs can be authenticated (for example, adding the APs to static users) when NAC authentication is deployed for users. Otherwise, the wireless users cannot be authenticated.
- For S5731-S, S5731S-S, S5720I-SI, S5720-LI, and S5720S-LI, the priority of a traffic policy is higher than that of an authentication policy. As a result, users may be able to access the network before being authenticated.
- NAC authentication cannot be enabled both on a Layer 2 Ethernet interface and the VLANIF interface mapping the VLAN of the Ethernet interface. Otherwise, the users have no network access rights after connecting to the network. In wireless scenarios, NAC authentication cannot be enabled both in VAP profiles and on VLANIF interfaces. In direct forwarding mode, NAC authentication configured on a VLANIF interface takes effect only when the device is connected in off-path mode.
- After enabling NAC on an interface, you cannot run the following commands on the interface. Similarly, after running the following commands on an interface, you cannot enable NAC on the interface.

Command	Function
mac-limit	Sets the maximum number of MAC addresses that can be learned by an interface.

Command	Function
mac-address learning disable	Disables MAC address learning on an interface.
port link-type dot1q-tunnel	Sets the link type of an interface to QinQ.
port vlan-mapping vlan map-vlan **port vlan-mapping vlan inner-vlan**	Configures VLAN mapping on an interface.
port vlan-stacking	Configures selective QinQ.
mac-vlan enable	Enables MAC address-based VLAN assignment on an interface.
ip-subnet-vlan enable	Enables IP subnet-based VLAN assignment on an interface.
user-bind ip sticky-mac	Enables the device to generate snooping MAC entries.

- After the encapsulation mode of packets allowed to pass a Layer 2 sub-interface is set to default using the **encapsulation** command, NAC cannot be configured on the main interface of the Layer 2 sub-interface.
- After NAC is configured on the main interface, the **bridge-domain (Layer 2 sub-interface view)** command cannot be executed on its Layer 2 sub-interface to associate with BDs. Similarly, NAC cannot be executed on the main interface if the **bridge-domain (Layer 2 sub-interface view)** command is configured on its Layer 2 sub-interface to associate with BDs.

Example

Apply the authentication profile **m1** to VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name m1
[HUAWEI-authen-profile-m1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] authentication-profile m1
```

13.5.70 authentication-profile (system view)

Function

The **authentication-profile** command creates an authentication profile and displays the authentication profile view.

The **undo authentication-profile** command deletes the authentication profile.

By default, the device has six built-in authentication profiles: default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile.

Format

authentication-profile name *authentication-profile-name*

undo authentication-profile name *authentication-profile-name*

Parameters

Parameter	Description	Value
name *authentication-profile-name*	Specifies the name of an authentication profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NAC can implement access control on users. The device uses authentication profiles to uniformly manage NAC configuration so that users can easily configure NAC functions. The parameters (for example, the bound access profile and authentication type) in the authentication profile can be configured to provide various access control modes for different users. After the configuration is complete, the authentication profile is applied to the interface or VAP profile to enable NAC.

Follow-up Procedure

1. Configuring authentication profiles: Configure the access profile, and authorization information in the authentication profiles.
2. Applying authentication profiles: Run the authentication-profile **(Interface view or VAP profile view)** command to apply the authentication profiles to the interface or VAP profile.

Precautions

- The built-in authentication profile **default_authen_profile** and the compatibility profile converted after an upgrade are not counted in the configuration specification. The six built-in authentication profiles (default_authen_profile, dot1x_authen_profile, mac_authen_profile,

portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile) can be modified and applied, but cannot be deleted.

- Before deleting an authentication profile, ensure that this profile is not bound to any interface or VAP profile. You can run the **display authentication-profile configuration** command to check whether the authentication profile is bound to an interface or VAP profile

Example

Create the authentication profile named **mac_authen_profile1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name mac_authen_profile1
```

13.5.71 band-width share-mode

Function

The **band-width share-mode** command enables the bandwidth share mode.

The **undo band-width share-mode** command restores the default configuration.

By default, the bandwidth share mode is disabled.

NOTE

This command is only supported by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

band-width share-mode

undo band-width share-mode

Parameters

None

Views

System view, AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On a home network, all family members go online using the same account. To improve service experience of family members, you can enable the bandwidth share mode so that all members can share the bandwidth.

Precautions

- This function is not supported in the direct forwarding mode of wireless traffic.
- If this command is run in the system view, it takes effect for all new online users who connected to the device. If this command is run in the AAA domain view, it takes effect only for new online users in the domain.
- If the local or remote RADIUS server does not assign CAR settings to the users who will go online and the online users, the share mode is invalid to the users.
- If the bandwidth share mode is enabled and different users use the same account for authentication, the users going online with no CAR settings assigned will not be affected when CAR settings are assigned to the users who go online later.

Example

Enable the bandwidth share mode in the system view.

```
<HUAWEI> system-view
[HUAWEI] band-width share-mode
```

Enable the bandwidth share mode in the AAA domain view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] band-width share-mode
```

13.5.72 capwap fragment

Function

The **capwap fragment** command configures the rate for wireless packet fragmentation.

The **undo capwap fragment** command cancels the rate configuration for wireless packet fragmentation.

By default, the rate for wireless packet fragmentation is not configured.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this function.

Format

capwap fragment cir *cir-value* [**cbs** *cbs-value*]

undo capwap fragment

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through an interface.	The value is an integer ranging from 24 to 104857600, in kbit/s.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the committed volume of burst traffic that can pass through an interface.	The value is an integer ranging from 10000 to 134217728, in bytes. By default, the CBS is 125 times the CIR. If the CIR multiplied by 125 is less than 10000, the default CBS is 10000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In wireless scenarios, a large number of burst ultra-long packets (longer than 1500 bytes) may exist and exceed the device forwarding performance. To ensure correct packet forwarding in such cases, you can run the **capwap fragment** command to configure the rate for wireless packet fragmentation. If the rate is not configured, packets are fragmented at the maximum rate supported by the device.

Precautions

Limiting the rate for fragmenting wireless packets affects wireless packet forwarding performance.

Example

Set the CIR to 10000 kbit/s for wireless packet fragmentation.

```
<HUAWEI> system-view
[HUAWEI] capwap fragment cir 10000
```


13.5.73 capwap unknown-unicast

Function

The **capwap unknown-unicast** command configures the rate for forwarding unknown unicast packets in wireless scenarios.

The **undo capwap unknown-unicast** command restores the default rate for forwarding unknown unicast packets in wireless scenarios.

By default, the CIR is 1600000 kbit/s and the CBS is 250000 bytes for unknown wireless unicast packets.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this function.

Format

capwap unknown-unicast cir *cir-value* [**cbs** *cbs-value*]

undo capwap unknown-unicast

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through an interface.	The value is 0 or an integer ranging from 24 to 104857600, in kbit/s. The value 0 indicates that no rate limit is configured for forwarding unknown unicast packets in wireless scenarios and these packets are forwarded at the maximum rate supported by the device.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the committed volume of burst traffic that can pass through an interface.	The value is an integer ranging from 10000 to 134217728, in bytes. By default, the CBS is 125 times the CIR. If the CIR multiplied by 125 is less than 10000, the default CBS is 10000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In wireless scenarios, a large number of burst unknown unicast packets may exist and exceed the device forwarding performance. To ensure correct packet replication and forwarding in such cases, you can run the **capwap unknown-unicast** command to configure the rate for forwarding unknown unicast packets.

Precautions

Limiting the rate for forwarding wireless unknown unicast packets affects wireless packet forwarding performance.

Example

Set the CIR to 2000000 kbit/s and the CBS to 300000 bytes for forwarding unknown wireless unicast packets.

```
<HUAWEI> system-view
[HUAWEI] capwap unknown-unicast cir 2000000 cbs 300000
```

13.5.74 cut access-user ucl-group

Function

The **cut access-user ucl-group** command forces UCL group users offline.

Format

cut access-user ucl-group { *group-index* | **name** *group-name* }

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The UCL group must exist.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

After a user goes online, if you want to modify the user's network access rights or detect that the user is unauthorized, run this command to force the user offline.

Example

Force UCL group users offline.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] cut access-user ucl-group name test
```

13.5.75 device-type

Function

The **device-type** command sets a terminal type identifier.

The **undo device-type** command deletes a terminal type identifier that has been set.

By default, no terminal type identifier exists in the system.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

device-type *device-name*

undo device-type

Parameters

Parameter	Description	Value
device-name	Specifies a terminal type identifier.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value cannot be - or --, and cannot contain ?, ', ".

Views

Terminal type identification profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a terminal type identifier is configured in a terminal type identification profile, the terminal type can be identified in the profile. Assume that the terminal type identifier is set to **test**. If the MAC address, user agent, or DHCP Option information that an AC receives from a terminal matches the identification rule configured in the terminal type profile, the terminal type is **test**. This helps administrators to perform access control and rights management for the terminal based on the identified terminal type.

Precautions

The **device-type** command is cyclic in nature, and only the latest configuration takes effect.

Example

In the terminal type identification profile **test**, configure the terminal type identifier **test_1**.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
[HUAWEI-device-profile-test] device-type test_1
```

13.5.76 device-profile

Function

The **device-profile** command creates a terminal type identification profile and enters the terminal type identification profile view, or directly enters the view of a terminal type identification profile that has already been created.

The **undo device-profile** command deletes a terminal type identification profile that has been created.

By default, no terminal type identification profile is created.

NOTE

This function is supported only by the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H and takes effect only for wireless access users.

Format

device-profile profile-name *profile-name*

undo device-profile { **all** | **profile-name** *profile-name* }

Parameters

Parameter	Description	Value
profile-name *profile-name*	Specifies the name of a terminal type identification profile.	The value is a string of 1 to 31 case-sensitive characters without characters including spaces and the following:/ \ : * ? " < > | @ ' %. The value cannot be - or --.
all	Deletes all terminal type identification profiles.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

With the development of Internet, many enterprises allow employees to wirelessly access the enterprise intranet using their own intelligent devices such as cellphones, tablets, and laptops, which satisfies employees' pursuit of new technology and desire of being unique, and improves their efficiency as well. This is called Bring Your Own Device (BYOD). However, access to enterprise intranet through PCs may cause potential security risks, and traditional security technology based on user identity authentication and authorization can no longer guarantee network security. It is in such a background that the terminal type identification technology comes out. With this technology, the types of the devices that employees use to access the intranet can be identified, facilitating access control. During the implementation of BYOD, administrators can limit intranet access rights to specified types of mobile devices and perform authentication and authorization based on users, device types, access time, access points, and environment information about the devices.

A terminal type identification profile is configured with terminal types that can be identified by devices, and identification rules. With the configured identification rules, the types of devices using which employees access the intranet can be identified, helping administrators to control employees' access rights.

Example

Create a terminal type identification profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
```


13.5.77 device-sensor dhcp option

Function

The **device-sensor dhcp option** command enables the DHCP-based terminal type awareness function.

The **undo device-sensor dhcp option** command disables the DHCP-based terminal type awareness function.

By default, the DHCP-based terminal type awareness function is disabled.

Format

device-sensor dhcp option *option-code* &<1-6>

undo device-sensor dhcp option *option-code* &<1-6>

Parameters

Parameter	Description	Value
option-code	Specifies the DHCP option field that the device needs to resolve. The option fields in a DHCP packet carry the control information and parameters, for example, terminal type.	The value is an integer that ranges from 1 to 254.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

After the DHCP-based terminal type awareness function is enabled, the device can resolve the option fields that carry terminal type information in the received DHCP Request packets. The device then sends the option information to the RADIUS server through RADIUS accounting packets. Through the option information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- To make this command take effect, you must run the **dhcp snooping enable** command on the interfaces or in VLANs.

Example

Set the option fields to be resolved by the device to option 60.

```
<HUAWEI> system-view
[HUAWEI] device-sensor dhcp option 60
```

13.5.78 device-sensor lldp tlv

Function

The **device-sensor lldp tlv** command enables the LLDP-based terminal type awareness function.

The **undo device-sensor lldp tlv** command disables the LLDP-based terminal type awareness function.

By default, the LLDP-based terminal type awareness function is disabled.

Format

device-sensor lldp tlv *tlv-type* &<1-4>

undo device-sensor lldp tlv

Parameters

Parameter	Description	Value
tlv-type	Specifies the LLDP TLV type as the terminal type to be aware of the device.	The value is an integer that can be 1, 2, 5, 6, 7, 8, and 127. The values are as follows: • 1: Chassis ID TLV, indicating the bridge MAC address of the device • 2: Port ID TLV, indicating the port identifying the LLD PDU sending end • 5: System Name TLV, indicating the device name • 6: System Description TLV, indicating the system description • 7: System Capabilities TLV, indicating the system capabilities • 8: Management Address TLV, indicating the management address • 127: Organization Specific TLV, indicating the user-defined organization information. You can run the **lldp tlv-enable med-tlv** command on the physical interface for user access to set this parameter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

Using the LLDP-based terminal type awareness function, the device parses the required TLV type containing terminal type information from the received LLDP packets. The device then sends the TLV type information to the RADIUS server through a RADIUS accounting packet. Through the TLV type information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- The command takes effect only when the LLDP function is enabled on the device and the connected peer device.
- This command takes effect only when terminals connect to the device through physical interfaces, instead of logical interfaces such as Eth-Trunk interfaces.

Example

Enable the terminal type awareness function based on LLDP TLV type 5.

```
<HUAWEI> system-view
[HUAWEI] device-sensor lldp tlv 5
```

13.5.79 device-sensor cdp tlv

Function

The **device-sensor cdp tlv** command enables the CDP-based terminal type awareness function.

The **undo device-sensor cdp tlv** command disables the CDP-based terminal type awareness function.

By default, the CDP-based terminal type awareness function is disabled.

Format

device-sensor cdp tlv *tlv-type* &<1-6>

undo device-sensor cdp tlv

Parameters

Parameter	Description	Value
tlv-type	Specifies the CDP TLV type as the terminal type to be aware of the device.	The value is an integer that can be 1, 2, 3, 4, 5, and 6. The values are as follows • 1: Device ID TLV, indicating a device ID. • 2: Address TLV, indicating the address of the interface that sends CDP packets. • 3: Port ID TLV, indicating the ID of the interface that sends CDP packets. • 4: Function TLV, indicating the device function. • 5: Version TLV, indicating the software version. • 6: Platform, indicating the hardware platform.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

Using the CDP-based terminal type awareness function, the device parses the required TLV type containing terminal type information from the received CDP packets. The device then sends the TLV type information to the RADIUS server through a RADIUS accounting packet. Through the TLV type information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- The command takes effect only when the CDP function is enabled on the device and the connected peer device.
- This command takes effect only when terminals connect to the device through physical interfaces, instead of logical interfaces such as Eth-Trunk interfaces.

Example

Enable the terminal type awareness function based on CDP TLV type 5.

```
<HUAWEI> system-view
[HUAWEI] device-sensor cdp tlv 5
```

13.5.80 display aaa statistics access-type-authenreq

Function

The **display aaa statistics access-type-authenreq** command displays the number of requests for MAC, Portal, or 802.1X authentication.

Format

display aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, or 802.1X authentications.

To view the number of requests for MAC, Portal, or 802.1X authentication, run the **display aaa statistics access-type-authenreq** command.

Example

Display the number of requests for MAC, Portal, or 802.1X authentication.

```
<HUAWEI> display aaa statistics access-type-authenreq
mac     authentication request     :2
portal  authentication request     :0
dot1x   authentication request     :0
```

Table 13-41 Description of the **display aaa statistics access-type-authenreq** command output

Item	Description
mac authentication request	Number of MAC authentication requests.
portal authentication request	Number of Portal authentication requests.
dot1x authentication request	Number of 802.1X authentication requests.

13.5.81 display access-context profile

Function

The **display access-context profile** command displays the configuration of a user context profile.

Format

display access-context profile [**name** *profile-name*]

Parameters

Parameter	Description	Value
name *profile-name*	Displays the configuration of the user context profile with a specified name. If **name** *profile-name* is not specified, all user context profiles configured on the device are displayed.	The value must be the name of an existing user context profile on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a user context profile, you can run this command to check whether the configuration is correct.

Example

Display all user context profiles configured on the device.

```
<HUAWEI> display access-context profile
-------------------------------------------------------------------------------
  ID       Access-context profile name
-------------------------------------------------------------------------------
   0       p1
   1       aA
-------------------------------------------------------------------------------
  Total 2, printed 2
```

Display the configuration of the user context profile **p1**.

```
<HUAWEI> display access-context profile name p1
 Profile name              : p1
 if-match vlan-id          : 13 to 20
```

Table 13-42 Description of the **display access-context profile** command output

Item	Description
ID	Index of a user context profile.
Access-context profile name or Profile name	Name of a user context profile. To configure the parameter, run the **access-context profile name** command.

Item	Description
if-match vlan-id	VLAN matching a user context profile. To configure the parameter, run the **if-match vlan-id** command.

13.5.82 display access-author policy

Function

The **display access-author policy** command displays the configuration of a user authentication event authorization policy.

Format

display access-author policy [**name** *policy-name*]

Parameters

Parameter	Description	Value
name *policy-name*	Displays the configuration of the user authentication event authorization policy with a specified name. If **name** *policy-name* is not specified, all user authentication event authorization policies configured on the device are displayed.	The value must be the name of an existing user authentication event authorization policy on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a user authentication event authorization policy, you can run this command to check whether the configuration is correct.

Example

Display all user authentication event authorization policies configured on the device.

```
<HUAWEI> display access-author policy
--------------------------------------------------------------------------------
```



```
  ID       Access-author policy name
------------------------------------------------------------------------------
   0       a1
   1       a2
------------------------------------------------------------------------------
  Total 2, printed 2
```

Display the configuration of the user authentication event authorization policy **a1**.

```
<HUAWEI> display access-author policy name a1
 Policy name              : a1
 match access-context-profile p1 action authen-fail service-scheme s1
```

Table 13-43 Description of the **display access-author policy** command output

Item	Description
ID	Index of a user authentication event authorization policy.
Access-author policy name or Policy name	Name of a user authentication event authorization policy. To configure the parameter, run the **access-author policy name** command.
match access-context-profile *profile-name* action authen-fail service-scheme *scheme-name*	User authorization information specified based on a user context profile. To configure the parameter, run the **match access-context-profile action** command.

13.5.83 display access-user

Function

The **display access-user** command displays information about NAC access users.

Format

display access-user service-scheme *service-scheme*

display access-user access-type static

display access-user access-type { **dot1x** | **mac-authen** | **portal** | **none** } [**wired** | **wireless**]

display access-user event { **pre-authen** | **authen-fail** | **client-no-response** | **authen-server-down** }

display access-user ucl-group { *group-index* | **name** *ucl-group-name* } [**detail**]

display access-user option82 { **circuit-id** *text* | **remote-id** *text* }

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **wireless** parameter.

Parameters

Parameter	Description	Value
service-scheme *service-scheme*	Displays information about users assigned with a specified service scheme.	The value must be the name of an existing service scheme.
access-type	Displays information about users using a specified authentication mode.	-
dot1x	Displays information about users who pass 802.1X authentication.	-
mac-authen	Displays information about users who pass MAC address authentication.	-
portal	Displays information about users who pass Portal authentication.	-
none	Displays information about users whose AAA scheme is non-authentication.	-
static	Displays static user information.	-
event	Displays information about users in a specified authentication phase.	-
pre-authen	Displays information about users in the pre-connection phase.	-

Parameter	Description	Value
authen-fail	Displays information about users who fail to be authenticated and are assigned network access policies when the authentication server sends authentication failure packets to the device.	-
client-no-response	Displays information about 802.1X authentication users who fail to be authenticated and are assigned network access policies when the 802.1X client does not respond.	-
authen-server-down	Displays information about users who fail to be authenticated due to the Down status of the authentication server and are assigned network access policies.	-
ucl-group	Displays information about users in a specified UCL group.	-
group-index	Specifies the index of a UCL group.	The value must be an existing UCL group index.
name *ucl-group-name*	Specifies the name of a UCL group.	The value must be an existing UCL group name.
detail	Displays detailed user information.	-
option82	Displays information about MAC address authentication users who use the Option 82 field as user names.	-
circuit-id *text*	Displays information about MAC address authentication users who specify the circuit ID as user names.	The value must be existing circuit-id information.

Parameter	Description	Value
remote-id *text*	Displays information about MAC address authentication users who specify the remote ID as user names.	The value must be existing remote-id information.
wired	Displays information about wired users.	-
wireless	Displays information about wireless users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about online NAC users.

Example

Display information about users who are assigned the service scheme **test**.

```
<HUAWEI> display access-user service-scheme test
--------------------------------------------------------------------------------
UserID Username              IP address      MAC            Status
--------------------------------------------------------------------------------
16018  zqm                  10.12.12.254    00e0-fcc2-0175 Pre-authen
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display information about users in the pre-connection phase.

```
<HUAWEI> display access-user event pre-authen
--------------------------------------------------------------------------------
UserID Username              IP address      MAC            Status
--------------------------------------------------------------------------------
16018  zqm                  10.12.12.254    00e0-fcc2-0175 Pre-authen
--------------------------------------------------------------------------------
Total: 1, printed: 1
```


NOTE

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

When you run the **display access-user** command without specifying any parameter to view user information and the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following the 19th character; that is, only 22 characters are displayed. When you run the **display access-user** command with parameters specified to view detailed information about the user table, all the characters of **username** are displayed, and the rule for converting special characters remains unchanged.

Table 13-44 Description of the **display access-user** command output

Item	Description
UserID	ID automatically allocated to an online user by the device.
Username	User name.
IP address	User IP address. When both IPv4 and IPv6 addresses exist, only the IPv4 address is recorded. When only IPv6 addresses exist, only the latest updated IPv6 address is recorded.
MAC	User MAC address.
Status	User status. ● Open: For a wired user, the user goes online through the open function upon authentication failure. For wireless users, no authentication is performed. ● Success: authentication is successful ● Pre-authen: pre-authentication ● Client-no-resp: the client does not respond ● Fail-authorized: authorization upon authentication failure ● Web-server-down: web server is Down ● Aaa-server-down: AAA server is Down

13.5.84 display access-user dot1x-identity statistics

Function

The **display access-user dot1x-identity statistics** command displays statistics about Identity packets for 802.1X authentication on a switch.

Format

display access-user dot1x-identity statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view the statistics about Identity packets for 802.1X authentication on a switch.

Example

Display statistics about Identity packets for 802.1X authentication on the switch.

```
<HUAWEI> display access-user dot1x-identity statistics
------------------------------------------------------------------------
Receive(Packet)    Pass(Packet)    Drop(Packet)    Last-dropping-time
------------------------------------------------------------------------
0                  0               0               -
------------------------------------------------------------------------
```

Table 13-45 Description of the **display access-user dot1x-identity statistics** command output

Item	Description
Receive(Packet)	Total number of Identity packets for 802.1X authentication received by the switch.
Pass(Packet)	Number of Identity packets for 802.1X authentication sent to and processed by the CPU of the switch.
Drop(Packet)	Number of Identity packets for 802.1X authentication discarded by the switch.

Item	Description
Last-dropping-time	Latest time when the switch discarded Identity packets for 802.1X authentication. If no packet loss record exists on the switch, this field displays **-**.

13.5.85 display access-user https statistics

Function

The **display access-user https statistics** command displays statistics about HTTPS protocol packets sent to the CPU.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display access-user https statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display statistics about HTTPS protocol packets sent to the CPU.

```
<HUAWEI> display access-user https statistics
------------------------------------------------------------------------------
Received packets:
   Tcp-syn:519

Passed packets:
   Tcp-syn:391
```



```
Dropped packets:
  Last dropping time:2019-03-12 09:26:46
  Duplicate tcp-syn within 1 second:0
  Rate-limited packets:128
```

Table 13-46 Description of the **display access-user https statistics** command output

Item	Description
Received packets: Tcp-syn	Number of HTTPS TCP handshake packets received by the switch.
Passed packets: Tcp-syn	Number of HTTPS TCP handshake packets sent to the CPU on the switch.
Dropped packets	Number of HTTPS TCP handshake packets dropped by the switch.
Last dropping time	Number of latest HTTPS TCP handshake packets dropped by the switch. If - is displayed, packet loss did not occur on the switch.
Duplicate tcp-syn within 1 second	Number of duplicate TCP handshake packets dropped by the switch within 1 second.
Rate-limited packets	Number of TCP handshake packets dropped by the switch due to rate limiting.

13.5.86 display access-user portal statistics

Function

The **display access-user portal statistics** command displays statistics about Portal protocol packets sent to the CPU.

Format

display access-user portal statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display statistics about Portal protocol packets sent to the CPU.

```
<HUAWEI> display access-user portal statistics
------------------------------------------------------------------------------
Receive(Packet)     Pass(Packet)     Drop(Packet)     Last-dropping-
time
------------------------------------------------------------------------------
0                   0                0                -
------------------------------------------------------------------------------
...
```

Table 13-47 Description of the **display access-user portal statistics** command output

Item	Description
Receive(Packet)	Total number of Portal protocol packets received by the switch.
Pass(Packet)	Number of Portal protocol packets sent to the CPU.
Drop(Packet)	Number of Portal protocol packets discarded by the switch.
Last-dropping-time	Last time when the switch discards Portal protocol packets. If no Portal protocol packet is discarded, this parameter is displayed as **-**.

13.5.87 display access-user roam-table

Function

The **display access-user roam-table** command displays the roaming table information of a roaming user.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command.

Format

display access-user roam-table [**mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **acct-session-id** *acct-session-id*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Displays the roaming table information of a roaming user with a specified MAC address.	The value is in the H-H-H format, where H is a 4-digit hexadecimal number.
ip-address *ip-address*	Displays the roaming table information of a roaming user with a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays the roaming table information of a roaming user with a specified IP address in a specified VPN instance.	The value must be an existing VPN instance name on the device.
acct-session-id *acct-session-id*	Displays the roaming table information of a roaming user with a specified accounting ID.	The value must be the current accounting ID of the user. For details, run the **display access-user user-id** *user-id* command to check the **User accounting session ID** field.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a user roams between different ACs, the user roaming table is generated on the AC (authentication point) before the user is re-authenticated. You can run this command to view the user roaming table information.

Precautions

In 802.1X authentication and MAC address authentication, roaming tables are generated only for accounting users, not non-accounting users.

Example

Display the roaming table information of a roaming user.


```
<HUAWEI> display access-user roam-table
 ------------------------------------------------------------------------------
 MAC            IP address                FAC address
------------------------------------------------------------------------------
 00e0-fc12-3456  10.1.1.2                   10.137.213.119
 ------------------------------------------------------------------------------
<HUAWEI> display access-user roam-table ip-address 10.1.1.2
  User MAC                        : 00e0-fc12-3456
  User accounting session ID            : AP6050-00000000000102fa****0000023
  User IP address                 : 10.1.1.2
  IP address of foreign AC              : 10.137.213.119
```

Table 13-48 Description of the **display access-user roam-table** command output

Item	Description
User accounting session ID	User accounting ID.
IP address/User IP address	User IP address.
MAC/User MAC	User MAC address.
FAC address/IP address of foreign AC	IP address of the AC where the user roams.

13.5.88 display access-user-num

Function

The **display access-user-num** command displays the number of current online users on a virtual access point (VAP).

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

display access-user-num [**interface wlan-dbss** *wlan-dbss-interface-id*]

Parameters

Parameter	Description	Value
interface wlan-dbss *wlan-dbss-interface-id*	Displays the number of current online users on a VAP. If this parameter is not specified, the number of current online users on all VAPs are displayed.	The value is an existing WLAN-DBSS interface id.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display access-user-num** command to view the number of current online users.

Example

Display the number of current online users on all VAPs.

```
<HUAWEI> display access-user-num
2016-09-30 11:09:27.790
--------------------------------------------------------------------------------
 Interface name                                  online-user-num
--------------------------------------------------------------------------------
 Wlan-Dbss0                                                  10
 Wlan-Dbss1                                                   0
--------------------------------------------------------------------------------
 Total: 8, printed: 2
```

Table 13-49 Description of the **display access-user-num** command output

Item	Description
Interface name	WLAN-DBSS interface id.
online-user-num	Number of current online users.
Total	Total number of interfaces.
printed	Number of printed entries.

13.5.89 display ap port-auth-state

Function

The **display ap port-auth-state** command displays the authentication status of an 802.1X client.

NOTE

This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Format

display ap port-auth-state { **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the authentication status of an 802.1X client with the specified AP name.	The AP name must already exist.
ap-id *ap-id*	Displays the authentication status of an 802.1X client with the specified AP ID.	The AP ID must already exist.
ap-mac *ap-mac*	Displays the authentication status of an 802.1X client with the specified AP MAC address.	The AP MAC address must already exist.
all	Displays the authentication status of all APs that are authenticated as 802.1X clients.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When an AP is authenticated as an 802.1X client, you can run this command to check the authentication status of the AP.

Example

Display the authentication status of all APs that are authenticated as 802.1X clients.

```
<HUAWEI> display ap port-auth-state all
------------------------------------------------------------------------------
AP-ID Port       Dot1x client State
------------------------------------------------------------------------------
23    GE0        init
------------------------------------------------------------------------------
Printed: 1
```

Table 13-50 Description of the **display ap port-auth-state** command output

Item	Description
AP-ID	AP ID.
Port	Port number.

Item	Description
Dot1x client State	Authentication status of an 802.1X client. • init: initial • authenticating: authenticating • success: succeeded • fail: failed

13.5.90 display authentication mac-move configuration

Function

The **display authentication mac-move configuration** command displays the MAC address migration configuration.

Format

display authentication mac-move configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display authentication mac-move configuration** command to view the MAC address migration configuration. The configuration includes the number of times that MAC address migration users are allowed to migrate their MAC addresses 60s before they enter the quiet state, the period that MAC address migration users stay in the quiet state, the interval at which a device detects users' online status before user MAC address migration, and the number of detections before user MAC address migration.

Example

Display the MAC address migration configuration.

```
<HUAWEI> display authentication mac-move configuration
Mac-move vlan config:all
Mac-move quiet times:1
Mac-move quiet period(s):120
Mac-move quiet log:ENABLE
```



```
Mac-move quiet user alarm:ENABLE
Mac-move quiet user alarm lower percentage(%):
50
Mac-move quiet user alarm upper percentage(%):100
Mac-move detect:DISABLE
Mac-move detect retry-interval(s):3
Mac-move detect retry-time:1
```

Table 13-51 Description of the **display authentication mac-move configuration** command output

Item	Description
Mac-move vlan config	VLAN ID range in which MAC address migration is enabled. For details, see the **authentication mac-move enable** command.
Mac-move quiet times	Number of times that MAC address migration users are allowed to migrate their MAC addresses 60s before they enter the quiet state. For details, see the **authentication mac-move quiet-times quiet-period** command.
Mac-move quiet period(s)	Period that MAC address migration users stay in the quiet state. For details, see the **authentication mac-move quiet-times quiet-period** command.
Mac-move quiet log	Whether a device is enabled to record logs about user quietness triggered by MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move quiet-log enable** command.
Mac-move quiet user alarm	Whether a device is enabled to send alarms about user quietness triggered by MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move quiet-user-alarm enable** command.

Item	Description
Mac-move quiet user alarm lower percentage(%)	Lower alarm threshold for the percentage of MAC address migration users in quiet state. For details, see the **authentication mac-move quiet-user-alarm percentage** command.
Mac-move quiet user alarm upper percentage(%)	Upper alarm threshold for the percentage of MAC address migration users in quiet state. For details, see the **authentication mac-move quiet-user-alarm percentage** command.
Mac-move detect	Whether a device is enabled to detect users' online status before user MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move detect enable** command.
Mac-move detect retry-interval(s)	Interval at which a device detects users' online status before user MAC address migration. For details, see the **authentication mac-move detect retry-interval retry-time** command.
Mac-move detect retry-time	Number of detections before user MAC address migration. For details, see the **authentication mac-move detect retry-interval retry-time** command.

13.5.91 display authentication mac-move quiet-user

Function

The **display authentication mac-move quiet-user** command displays information about MAC address migration users in quiet state.

Format

display authentication mac-move quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all MAC address migration users in quiet state.	-
mac-address *mac-address*	Displays information about MAC address migration users in quiet state with a specified MAC address.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run this command to view information about MAC address migration users in quiet state.

Example

Display information about all MAC address migration users in quiet state.

```
<HUAWEI> display authentication mac-move quiet-user all
Quiet MAC Information
--------------------------------------------------------------------------------
Quiet MAC                                Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
xxxx-xxxx-xxxx                           143
--------------------------------------------------------------------------------
1 quiet MAC found, 1 printed.
```

Table 13-52 Description of the **display authentication mac-move quiet-user all** command output

Item	Description
Quiet MAC	MAC address of MAC address migration users in quiet state.
Quiet Remain Time(Sec)	Remaining quiet time of MAC address migration users in quiet state, in seconds.

13.5.92 display authentication interface

Function

The **display authentication interface** command displays the configuration of the NAC authentication mode on an interface.

Format

display authentication interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the configuration of the NAC authentication mode on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the NAC authentication mode, you can run this command to check the configuration.

Example

Display the configuration of the NAC authentication mode on GE0/0/1.

```
<HUAWEI> display authentication interface gigabitethernet 0/0/1
Authentication profile: p1
Authentication access-point: Enable
Authentication access-point max-user: 10
Port authentication order:
                    MAC
                    DOT1X
                    WEB
```


Table 13-53 Description of the **display authentication interface** command output

Item	Description
Authentication profile	Name of the authentication profile applied to the interface.
Authentication access-point	Whether the interface functions as an access control point. **NOTE** This field is displayed only on access devices used in policy association solutions.
Authentication access-point max-user	Maximum number of users who are allowed to log in through an access point **NOTE** This field is displayed only on access devices used in policy association solutions.
Port authentication order	Authentication mode configured in the authentication profile applied to the interface. Authentication modes include: • MAC: indicates the MAC address authentication mode. • DOT1X: indicates the 802.1X authentication mode. • WEB: indicates the Portal authentication mode. **NOTE** • On a standalone device, if MAC address bypass authentication is enabled in the authentication profile using the **authentication dot1x-mac-bypass** command, **DOT1X** is displayed before **MAC**. If MAC address bypass authentication is disabled, **MAC** is displayed before **DOT1X**. • On an AS device in an SVF system or a policy association scenario, this item only indicates authentication modes configured in the authentication profile, and does not indicate the authentication sequence.

13.5.93 display authentication mode

Function

The **display authentication mode** command displays the current NAC configuration mode and the mode after restart.

Format

display authentication mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display authentication mode** command to view the current NAC configuration mode.

Example

Display the current NAC configuration mode and the mode after restart.

```
<HUAWEI> display authentication mode
  Current authentication mode is unified-mode
  Next authentication mode is unified-mode
```

Table 13-54 Description of the **display authentication mode** command output

Item	Description
Current authentication mode is unified-mode	Current NAC configuration mode.
Next authentication mode is unified-mode	NAC configuration mode after the device restarts. Run the **authentication unified-mode** command to switch the NAC mode to unified mode. Run the **undo authentication unified-mode** command to switch the NAC mode to common mode.

13.5.94 display authentication user-alarm configuration

Function

The **display authentication user-alarm configuration** command displays alarm thresholds for the percentage of successfully authenticated NAC users.

Format

display authentication user-alarm configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the alarm thresholds for the percentage of successfully authenticated NAC users.

Example

Display the alarm thresholds for the percentage of successfully authenticated NAC users.

```
<HUAWEI> display authentication user-alarm configuration
  Current Alarm Percent:100
  Current Alarm Resume Percent:60
```

Table 13-55 Description of the **display authentication user-alarm configuration** command output

Item	Description
Current Alarm Percent	Upper alarm threshold for the percentage of successfully authenticated NAC users.
Current Alarm Resume Percent	Lower alarm threshold for the percentage of successfully authenticated NAC users.

13.5.95 display authentication-profile configuration

Function

The **display authentication-profile configuration** command displays the configuration of an authentication profile.

Format

display authentication-profile configuration [**name** *authentication-profile-name*]

Parameters

Parameter	Description	Value
name *authentication-profile-name*	Displays the configuration of a specified authentication profile. If **name** *authentication-profile-name* is not specified, the device displays all the authentication profiles configured on the device.	The value must be the name of an existing authentication profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an authentication profile, you can run this command to check whether the configuration is correct.

NOTE

The built-in authentication profile **default_authen_profile** is not counted in the configuration specification. The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is also not counted in the configuration specification.

Example

Display all the authentication profiles configured on the device.

```
<HUAWEI> display authentication-profile configuration
-------------------------------------------------------------------------------
  ID      Auth-profile name
-------------------------------------------------------------------------------
  0       default_authen_profile
  1       dot1x_authen_profile
  2       mac_authen_profile
  3       portal_authen_profile
  4       dot1xmac_authen_profile
  5       multi_authen_profile
  6       p1
-------------------------------------------------------------------------------
  Total 7, printed 7
```


Table 13-56 Description of the **display authentication-profile configuration** command output

Item	Description
ID	Authentication profile ID.
Auth-profile name	Authentication profile name.

Display the configuration of the authentication profile **p1**.

```
<HUAWEI> display authentication-profile configuration name p1
  Profile name                              : p1
  Dot1x access profile name                 : -
  Mac access profile name                   : -
  Portal access profile name                : testdel
  Free rule template                        : -
  Force domain                              : -
  Dot1x force domain                        : -
  Mac-authen force domain                   : -
  Portal force domain                       : -
  Default domain                            : 110
  Dot1x default domain                      : -
  Mac-authen default domain                 : -
  Portal default domain                     : -
  Permit domain                             : -
  Authentication handshake                  : Enable
  Authentication handshake period           : 300s
  Auth-fail re-auth period                  : 60s
  Pre-auth Re-auth period                   : 60s
  Auth-fail re-auth period wlan-user        : 0s
  Auth-fail aging time                      : 82800s
  Pre-auth aging time                       : 82800s
  Author-keep aging time                    : 0s
  Dot1x-mac-bypass                          : Disable
  Mac authen before 802.1x authen force     : Enable
  Mac authen before 802.1x authen           : Enable
  Single-access                             : Disable
  Device-type authorize service-scheme      : -
  Iconnect device authorize service-scheme  : example_iconnect
  Mac move detect enable                    : Enable
  Authentication mode                       : multi-authen
  Authen-fail authorize service-scheme      : -
  Authen-server-down authorize service-scheme : -
  Authen-server-down authorize keep         : response-success
  Authen-server-noreply authorize keep      : response-success
  Authen-server-down close re-authen        : N
  Pre-authen authorize service-scheme       : -
  Security-name-delimiter                   : -
  Domain-name-delimiter                     : -
  Domain-location                           : -
  Domainname-parse-direction                : -
  Bound vap profile                         : -
  SVF flag                                  : Disable
  Ip-static-user                            : Disable
  Roam-realtime-accounting                  : Enable
  Update-IP-realtime-accounting             : Enable
  IP-address in-accounting-start            : Enable
  IPv4-address in-accounting-start mandatory : Enable
  Linkdown offline delay time               : 10
  Termination action                        : reauthenticate
  Control direction                         : Inbound
  Redirect ACL original url                 : Enable
  Update-Info-realtime-accounting           : Enable
  IPv6 Control Flag                         : N
  No IP Check Flag                          : N
```



```
IP Conflict Check Flag                    : Y
Authentication roam pre-authen mac-authen   : Enable
Authentication single-stack-control enable  : IPv6
Authentication no-replace dot1x             : -
Lldp sensor-ap authentication disable       : Disable
Drop dhcp-packet user-no-online             : Enable
```

Table 13-57 Description of the **display authentication-profile configuration name** command output

Item	Description
Profile name	Authentication profile name.
Dot1x access profile name	802.1X access profile bound to the authentication profile. To bind an 802.1X access profile, run the **dot1x-access-profile** command in the authentication profile view.
Mac access profile name	MAC access profile bound to the authentication profile. To bind a MAC access profile, run the **mac-access-profile** command in the authentication profile view.
Portal access profile name	Portal access profile bound to the authentication profile. To bind a Portal access profile, run the **portal-access-profile** command in the authentication profile view.
Free rule template	Authentication-free rule profile bound to the authentication profile. To bind an authentication-free rule profile, run the **free-rule-template** command in the authentication profile view.
Force domain	Forcible domain for users. To configure a forcible domain, run the **access-domain** command.
Dot1x force domain	Forcible domain for 802.1X authentication users. To configure a forcible domain for 802.1X authentication users, run the **access-domain** command.
Mac-authen force domain	Forcible domain for MAC address authentication users. To configure a forcible domain for MAC address authentication users, run the **access-domain** command.

Item	Description
Portal force domain	Forcible domain for Portal authentication users. To configure a forcible domain for Portal authentication users, run the **access-domain** command.
Default domain	Default domain for users. To configure a default domain for users, run the **access-domain** command.
Dot1x default domain	Default domain for 802.1X authentication users. To configure a default domain for 802.1X authentication users, run the **access-domain** command.
Mac-authen default domain	Default domain for MAC address authentication users. To configure a default domain for MAC address authentication users, run the **access-domain** command.
Portal default domain	Default domain for Portal authentication users. To configure a default domain for Portal authentication users, run the **access-domain** command.
Permit domain	Permitted domain for users. To configure a permitted domain, run the **permit-domain** command.
Authentication handshake	Whether the handshake function is enabled. ● Enable ● Disable To enable the handshake function, run the **authentication handshake** command.
Authentication handshake period	Handshake interval. To configure a handshake interval, run the **authentication timer handshake-period** command.

Item	Description
Auth-fail re-auth period	Interval for re-authenticating wired users who fail to be authenticated. To configure the interval, run the **authentication timer re-authen** command.
Pre-auth re-auth period	Interval for re-authenticating pre-connection users. To configure the interval, run the **authentication timer re-authen** command.
Auth-fail re-auth period wlan-user	Interval for re-authenticating wireless users who fail to be authenticated. To configure the interval, run the **authentication timer re-authen** command.
Auth-fail aging Time	Aging time for entries of the users who fail to be authenticated. To configure the aging time, run the **authentication timer authen-fail-aging** command.
Pre-auth aging Time	Aging time for pre-connection user entries. To configure the aging time, run the **authentication timer pre-authen-aging** command.
Author-keep aging time	Aging time for entries of online users who are authorized to retain the original network access rights. To configure the aging time, run the **authentication timer authorize-keep-aging** command.
Dot1x-mac-bypass	Whether MAC address bypass authentication is enabled. ● Enable ● Disable To configure the function, run the **authentication dot1x-mac-bypass** command.

Item	Description
Mac authen before 802.1x authen force	Whether forcible MAC address authentication is enabled before 802.1X authentication. • Enable • Disable To enable the function, run the **authentication mac-authen-first force** command.
Mac authen before 802.1x authen	Whether the sequence of authentication modes triggered by EAP-Start packets is configured to be MAC address authentication prior to 802.1X authentication. • Enable • Disable To configure this function, run the **authentication order mac dot1x** command.
Single-access	Whether the device allows users to access in only one authentication mode. To configure the function, run the **authentication single-access** command.
Device-type authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to voice terminals that are not authenticated. To configure the name, run the **authentication device-type voice authorize** command.
Iconnect device authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to iConnect terminals that are not authenticated. To configure the name, run the **authentication device-type iconnect authorize** command.
Authentication mode	User access mode. To configure the mode, run the **authentication mode** command.

Item	Description
Authen-fail authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to users who fail to be authenticated. To configure the name, run the **authentication event action authorize** command.
Authen-server-down authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to users when the authentication server is Down. To configure the name, run the **authentication event action authorize** command.
Authen-server-down authorize keep	The device retains the original network access rights of users and responds to users when the authentication server is Down. ● response-success: The device returns an authentication success packet to users. ● response-fail: The device returns an authentication failure packet to users. ● no-response: The device does not respond to users. To configure the function, run the **authentication event action authorize**.
Authen-server-noreply authorize keep	The device retains the original network access rights of users and responds to users when the authentication server does not respond. ● response-success: The device returns an authentication success packet to users. ● response-fail: The device returns an authentication failure packet to users. ● no-response: The device does not respond to users. To configure the function, run the **authentication event action authorize**.

Item	Description
Authen-server-down close re-authen	Whether to disable the re-authentication function when the authentication server is Down. ● Y ● N To configure the function, run the **authentication event authen-server-down action close re-authen**.
Pre-authen authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to users who are in the pre-connection state. To configure the name, run the **authentication event action authorize** command.
Security-name-delimiter	Security string delimiter. To configure the delimiter, run the **security-name-delimiter** command.
Domain-name-delimiter	Domain name delimiter. To configure the delimiter, run the **domain-name-delimiter** command.
Domain-location	Domain name location. To configure the location, run the **domain-location** command.
Domainname-parse-direction	Domain name resolution direction. To configure the direction, run the **domainname-parse-direction** command.
Bound vap profile	VAP profile to which the authentication profile is bound. To configure a VAP profile, run the **authentication-profile** command.
SVF flag	Whether SVF is enabled. ● Enable ● Disable
Ip-static-user	Whether the function of identifying static users through IP addresses is enabled. ● Enable ● Disable To configure the function, run the **ip-static-user enable** command.

Item	Description
Roam-realtime-accounting	Whether a device is enabled to send accounting packets during roaming. ● Enable ● Disable To configure the function, run the **authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command.
Update-IP-realtime-accounting	Whether a device is enabled to send accounting packets during address updating. ● Enable ● Disable To configure the function, run the **authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command.
Linkdown offline delay time	User logout delay when an interface link is faulty. To configure the delay, run the **link-down offline delay** command.
IP-address in-accounting-start	Whether the function of carrying users' IP addresses in accounting-start packets is enabled. ● Enable ● Disable To configure the function, run the **authentication ip-address in-accounting-start** command.
IPv4-address in-accounting-start mandatory	Whether the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets is enabled. ● Enable ● Disable To configure the function, run the **authentication ipv4-address in-accounting-start mandatory** command.

Item	Description
Termination action	Whether the device is configured to reauthenticate users when the time exceeds the value of Session-Timeout delivered by the RADIUS server. ● reauthenticate To configure the function, run the **authentication termination-action reauthenticate** command.
Control direction	Direction of packets controlled by the device. ● Inbound: Only upstream traffic is controlled. ● All: Bidirectional traffic is controlled. To configure the function, run the **authentication control-direction** command.
Redirect ACL original url	Whether the redirect URL is configured to carry the original URL when Portal-authenticated users who match a redirect ACL are forcibly redirected for another forcible Portal authentication. ● Enable ● Disable To configure the function, run the **authentication redirect-acl original-url enable** command.
Update-Info-realtime-accounting	Whether a device is enabled to send accounting packets for terminal information updates. ● Enable ● Disable To configure the function, run the **authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command.
IPv6 Control Flag	Whether network admission control is enabled for IPv6 users. ● Y: The function is enabled. ● N: The function is disabled. To configure the function, run the **authentication ipv6-control enable** command.

Item	Description
No IP Check Flag	Whether the device is enabled not to create any IP hash tables for the client IP address. ● Y ● N To configure the function, run the **authentication no-ip-check** command.
IP Conflict Check Flag	Whether the device is enabled not to check IP address conflicts for client IP addresses. ● Y ● N To configure the function, run the **authentication ip-conflict-check enable** command.
Authentication roam pre-authen mac-authen	Whether MAC address authentication is enabled for roaming STAs. ● Enable ● Disable To configure this function, run the **authentication roam pre-authen mac-authen enable** command.
Mac move detect enable	Whether the device is enabled to detect users' online status before user MAC address migration: ● Enable ● Disable To enable this function, run the **authentication mac-move detect enable** command.
Authentication single-stack-control enable	Whether the single-stack authentication function is enabled. ● IPv4 ● IPv6 ● Disable To configure the single-stack authentication function, run the **authentication single-stack-control enable** command.

Item	Description
Authentication no-replace dot1x	Whether the device is enabled not to respond to the EAP-Start packets sent from users who have successfully passed MAC address authentication or Portal authentication. ● dot1x: The function is enabled. ● -: The function is disabled. ● voice-device: The function is enabled and takes effect only for voice terminals. To configure this function, run the **authentication no-replace dot1x** command.
Lldp sensor-ap authentication disable	Whether the switch is enabled to allow Huawei LLDP-identified APs to access the network without authentication. ● Enable ● Disable To configure the function, run the **lldp sensor-ap authentication disable** command.
Drop dhcp-packet user-no-online	Whether to discard DHCP packets when 802.1x authentication users are offline or during re-authentication. ● Enable ● Disable To configure the function, run the **authentication drop dhcp-packet user-no-online enable** command.

13.5.96 display device-profile

Function

The **display device-profile** command displays the configuration of a specified terminal type identification profile or all terminal type identification profiles.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

display device-profile { **all** | **profile-name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays summary of all terminal type identification profiles.	-
profile-name *profile-name*	Displays detailed information about a specified terminal type identification profile.	The value must be the name of an existing terminal type identification profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring terminal type identification, you can run the **display device-profile** command to view the terminal type identification profile configuration, including the profile name, terminal type identifier, and ACL rule.

Example

Display summary of all terminal type identification profiles.

```
<HUAWEI> display device-profile all

-------------------------------------------------------------------------------

  Index     Name                        Device type                 Rule num
State

-------------------------------------------------------------------------------

  0       test                        example                   1           enable

-------------------------------------------------------------------------------

  Total count : 1
```

Display detailed information about the terminal type identification profile **test**.

```
<HUAWEI> display device-profile profile-name test
  ------------------------------------------------------------------------
  Name        : test
  Device type : example
  State       : disabled
  Rule        :
    rule 1 mac xxxx-xxxx-xxxx mask 12
  Match       :
    if-match rule id 1
  ------------------------------------------------------------------------
```


Table 13-58 Description of the **display device-profile** command output

Item	Description
Name	Name of a terminal type identification profile. To set a terminal type identification profile name, run the **device-profile** command.
Device type	Terminal type identifier. To set a terminal type identifier, run the **device-type** command.
Rule num	Number of ACL rules.
State	Whether to enable terminal type identification: • enable: Terminal type identification is enabled. • disabled: Terminal type identification is disabled. To enable terminal type identification, run the **enable** command.
Rule	Terminal identification rule. To set a terminal identification rule, run the **rule** command.
Match	Matching mode of terminal type identification rules. To set a matching mode of terminal type identification rules, run the **if-match** command.

13.5.97 display dot1x

Function

The **display dot1x** command displays 802.1X authentication information.

Format

display dot1x statistics

display dot1x [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
statistics	Displays statistics on 802.1X authentication. The statistics about 802.1X authentication is displayed only when this parameter is specified.	-
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays 802.1X authentication information of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. If this parameter is not specified, 802.1X authentication information of all interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display dot1x** command to view configuration results of all configuration commands in 802.1X authentication and statistics about 802.1X packets.

The command output helps you to check whether the current 802.1X authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

The **display dot1x** command displays the statistics on 802.1X packets. You can locate the fault according to the packet statistics. When the fault is rectified, run the **reset dot1x statistics** command to clear the packet statistics. After a period of time, run the **display dot1x** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

Display 802.1X authentication information.

```
<HUAWEI> display dot1x
 Max users: 10000
 Current users: 1
 Global default domain is jqq
 Dot1x abnormal-track cache-record-num: 20
 Quiet function is Disabled
 Mc-trigger port-up-send is Disabled
 Parameter set:Quiet Period               180s   Quiet-times          1
               Tx Period                  30s   Mac-By-Pass Delay    10s
 Dot1x URL: 123456


GigabitEthernet10/0/1Wlan-Dbss0 status: UP  802.1x protocol is Enabled
 Dot1x access profile is jqq
 Authentication mode is multi-authen
 Authentication method is EAP
 Reauthentication is enabled
 Reauthen period: 300s
 Dot1x retry times: 2
 Authenticating users: 0
 Current users: 0

 Authentication Success: 0          Failure: 0
 Enter Enquence        : 0
 EAPOL Packets: TX     : 68         RX     : 0
 Sent      EAPOL Request/Identity Packets  : 3
           EAPOL Request/Challenge Packets : 0
           Multicast Trigger Packets       : 64
           EAPOL Success Packets           : 0
           EAPOL Failure Packets           : 1
 Received  EAPOL Start Packets             : 0
           EAPOL Logoff Packets            : 0
           EAPOL Response/Identity Packets : 0
           EAPOL Response/Challenge Packets: 0

Online user(s) info:
UserId   MAC/VLAN           AccessTime             UserName
--------------------------------------------------------------------------------
1047     xxxx-xxxx-xxxx/27   2018/12/06 19:27:54     jqq
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display 802.1X statistics.


```
<HUAWEI> display dot1x statistics
 Dropped   EAPOL Access Flow Control       : 0
           EAPOL Check Sysmac Error        : 0
           EAPOL Get Vlan ID Error         : 0
           EAPOL Packet Flow Control       : 0
           EAPOL Online User Reach Max     : 0
           EAPOL Static or BlackHole Mac   : 0
           EAPOL Get Vlan Mac Error        : 0
           EAPOL Temp User Exist           : 0
           EAPOL no replace dot1x          : 0

 DHCP      Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 ARP       Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 ND        Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 DHCPv6    Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 ANYL2     Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 Sent      Authentication Request          : 0
           Cut Request                     : 0
           Cut Command Ack                 : 0
           Authentication Ack Fail Aff     : 0
           Update Ip                       : 0
           Wlan Eap Authentication Request     : 0
           Wlan Eap Authentication Request Ack : 0
           Wlan Eap Send Pmk               : 0
           Wlan Eap Reauthenticate Send Pmk    : 0
           Update User Online Time         : 0

 Received  Authentication Ack              : 0
           Reauthenticate Command          : 0
           Cut Command                     : 0
           Cut Ack                         : 0
           Sam Nac Ack                     : 0
           Notify Server Up                : 0
           Wlan Eap Authentication Request     : 0
           Wlan Mac Authentication Request     : 0
           Notify Vlanif Mac Authentication    : 0
```

Table 13-59 Description of the **display dot1x** command output

Item	Description
Max users	Maximum number of global online users, the value varies according to device models.
Current users	Number of current online users.
Global default domain is	Global default authentication domain. To configure the global default authentication domain, run the **domain** command.

Item	Description
Dot1x abnormal-track cache-record-num	Number of EAP packets for abnormal 802.1X authentication that can be recorded by the device. For details, see **dot1x abnormal-track cache-record-num**.
Quiet function is	Whether the quiet function is enabled. ● Enabled. ● Disabled. To configure the quiet function, run the **dot1x quiet-period** command.
Mc-trigger port-up-send is	Whether the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is enabled. ● Enabled. ● Disabled. To configure the function, run the **dot1x mc-trigger port-up-send enable** command.
Parameter set	Settings of 802.1X parameters: ● Quiet Period: specifies the quiet period set by the quiet timer. To configure the quiet period, run the **dot1x timer quiet-period** command. ● Quiet-times: specifies the maximum number of authentication failures before the device quiets a user. To configure the maximum value, run the **dot1x quiet-times** command. ● Tx Period: specifies the interval for sending authentication requests. To configure the interval, run the **dot1x timer tx-period** command. ● Mac-By-Pass Delay: specifies the value of the delay timer for MAC address bypass authentication.
Dot1x URL	Redirect-to URL for HTTP access of 802.1X users. To configure the redirect-to URL, run the **dot1x url** command.
interface status	Interface status: ● UP: The interface is enabled. ● DOWN: The interface is shut down.
802.1x protocol is	Whether 802.1X authentication is enabled on the interface. ● Enabled. ● Disabled.

Item	Description
Dot1x access profile is	802.1X access profile name. To configure the 802.1X access profile name, run the **dot1x-access-profile** command.
Authentication mode is	User access mode. To configure the user access mode, run the **authentication mode** command.
Authentication method is	Authentication mode of 802.1X users. To configure the authentication mode of 802.1X users, run the **dot1x authentication-method** command.
Reauthentication is	Whether re-authentication is enabled for online 802.1X users. To configure the function, run the **dot1x reauthenticate** command.
Dot1x retry times	Maximum number of attempts to send authentication requests to 802.1X users. To configure maximum number of attempts to send authentication requests to 802.1X users, run the **dot1x retry** command.
Authenticating users	Number of users who are being authenticated.
Current users	Number of online users on the interface.
Authentication Success	Number of successful authentications. The statistics include statistics on online 802.1X users but not on the users using MAC address bypass authentication.
Failure	Number of authentication failures. The statistics include statistics on online 802.1X users but not on the users using MAC address bypass authentication. The statistics do not include authentication failures caused by EAP-Request/Identity request timeouts and EAP-Request/MD5 Challenge request timeouts.
Enter Enquence	Number of packets entering the queue.
EAPOL Packets	Number of globally EAPOL packets. ● TX: Number of sent EAPOL packets. ● RX: Number of received EAPOL packets.
Sent	Statistics of sent packet.
EAPOL Request/ Identity Packets	Number of globally EAPOL Request/Identity packets.

Item	Description
EAPOL Request/ Challenge Packets	Number of globally EAPOL Request/Challenge packets.
Multicast Trigger Packets	Number of multicast packets that trigger authentication.
EAPOL Success Packets	Number of globally EAPOL Success packets.
EAPOL Failure Packets	Number of globally EAPOL Failure packets.
Received	Statistics of received packet.
EAPOL Start Packets	Number of globally EAPOL Start packets.
EAPOL Logoff Packets	Number of globally EAPOL LogOff packets.
EAPOL Response/ Identity Packets	Number of globally EAPOL Response/Identity packets.
EAPOL Response/ Challenge Packets	Number of globally EAPOL Response/Challenge packets.
Online user(s) info	Online user information: ● UserId: User ID. ● MAC/VLAN: MAC address/VLAN ID. ● AccessTime: Access time. ● UserName: User name. ● Total: Total number of online users. ● printed: Number of displayed online users.

Item	Description
Dropped	Number of discarded EAP packets. • EAPOL Access Flow Control: number of packets that are discarded because the user access rate is exceeded. • EAPOL Check Sysmac Error: number of packets that are discarded because the device MAC address is incorrect. • EAPOL Get Vlan ID Error: number of packets that are discarded because the obtained VLAN ID is incorrect. • EAPOL Packet Flow Control: number of packets that are discarded because the packet access rate is exceeded. • EAPOL Online User Reach Max: number of packets that are discarded because the number of online users reaches the maximum. • EAPOL Static or BlackHole Mac: number of packets that are discarded because the packet MAC address is a static MAC address or blackhole MAC address. • EAPOL Get Vlan Mac Error: number of packets that are discarded because the obtained VLAN MAC address is incorrect. • EAPOL Temp User Exist: number of packets that are discarded because the temporary user exists. • EAPOL no replace dot1x: number of EAP Start packets that are discarded due to 802.1X authentication of successfully authenticated MAC or Portal users.
DHCP	DHCP packet statistics.
ARP	ARP packet statistics.
ND	ND packet statistics.
DHCPv6	DHCPv6 packet statistics.
ANYL2	Any Layer 2 packet statistics.
Processed Packet	Number of processed packets.
Dropped Packet	Number of discarded packets.
Authentication Request	Number of authentication request messages.
Cut Request	Number of logout request messages.
Cut Command Ack	Number of acknowledgment messages to logout command request messages.
Authentication Ack Fail Aff	Number of the user is disconnected after the wireless user authentication fails.

Item	Description
Update Ip	Number of IP address update messages.
Wlan Eap Authentication Request	Number of EAP authentication request messages initiated by the WLAN module.
Wlan Eap Authentication Request Ack	Number of acknowledgment messages to EAP authentication request messages initiated by the WLAN module.
Wlan Eap Send Pmk	Number of PMK messages sent when the WLAN module performs EAP authentication.
Wlan Eap Reauthenticate Send Pmk	Number of PMK messages sent when the WLAN module performs EAP re-authentication.
Update User Online Time	Number of the user online time is updated.
Authentication Ack	Number of authentication acknowledgment messages.
Reauthenticate Command	Number of re-authentication messages.
Cut Command	Number of logout command request messages.
Cut Ack	Number of acknowledgment messages to logout request messages.
Sam Nac Ack	Number of EAP messages replied by the SAM module.
Notify Server Up	Number of RADIUS server Up messages.
Wlan Mac Authentication Request	Number of MAC authentication request messages initiated by the WLAN module.
Notify Vlanif Mac Authentication	Number of MAC authentication request messages of a VLANIF interface.

13.5.98 display dot1x-access-profile configuration

Function

The **display dot1x-access-profile configuration** command displays the configuration of an 802.1X access profile.

Format

display dot1x-access-profile configuration [**name** *access-profile-name*]

Parameters

Parameter	Description	Value
name *access-profile-name*	Displays the configuration of an 802.1X access profile with a specified name. If **name** *access-profile-name* is not specified, the device displays all the 802.1X access profiles configured on the device. If **name** *access-profile-name* is specified, the device displays the configuration of a specified 802.1X access profile.	The value must be the name of an existing 802.1X access profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an 802.1X access profile, you can run this command to check whether the configuration is correct.

NOTE

The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is not counted in the configuration specification.

Example

Display all the 802.1X access profiles configured on the device.

```
<HUAWEI> display dot1x-access-profile configuration
--------------------------------------------------------------------------------
ID          Dot1x-Access-Profile Name
--------------------------------------------------------------------------------
0           dot1x_access_profile
1           d1
2           d2
3           d3
4           d4
--------------------------------------------------------------------------------
Total: 5 printed: 5.
```


Table 13-60 Description of the **display dot1x-access-profile configuration** command output

Item	Description
ID	802.1X access profile ID.
Dot1x-Access-Profile Name	802.1X access profile name.

Display the configuration of the 802.1X access profile **d1**.

```
<HUAWEI> display dot1x-access-profile configuration name d1
  Profile Name                : d1
  Authentication method       : EAP
  Port control                : authorized-force
  Re-authen                   : Enable
  Client-no-response authorize : -
  Trigger condition           : arp
  Unicast trigger             : Enable
  Trigger dhcp-bind           : Enable
  Handshake                   : Disable
  Handshake packet-type       : request-identity
  Max retry value             : 2
  Reauthen Period             : 3600s
  Client Timeout              : 5s
  Handshake Period            : 60s
  Eth-trunk handshake period  : 120s
  Dot1x no-response authorize  : Disable
  Dot1x eap-success response   : Disable
  Bound authentication profile : -
```

Table 13-61 Description of the **display dot1x-access-profile configuration name** command output

Item	Description
Profile Name	802.1X access profile name.
Authentication method	Authentication mode of 802.1X users: ● CHAP ● PAP ● EAP To configure the authentication mode, run the **dot1x authentication-method** command.
Port control	802.1X authentication interface's authorization status: ● auto ● authorized-force ● unauthorized-force To set an authorization state for an interface, run the **dot1x port-control** command.

Item	Description
Re-authen	Whether re-authentication for online 802.1X users is enabled: ● Enable ● Disable To configure the re-authentication function, run the **dot1x reauthenticate** command.
Client-no-response authorize	Network access rights granted to users when the 802.1X client does not respond. ● service-scheme: The name of a service scheme based on which network access rights are assigned. ● ucl-group: The name of a UCL group based on which network access rights are assigned. ● vlan: The VLAN based on which network access rights are assigned. To configure the network access rights, run the **authentication event client-no-response action authorize** command.
Trigger condition	Packet type that can trigger 802.1X authentication: ● dhcp ● arp ● dhcpv6 ● nd ● any-l2-packet To configure the packet type, run the **authentication trigger-condition** (802.1X authentication) command.
Unicast trigger	Whether 802.1X authentication triggered by unicast packets is enabled: ● Enable ● Disable To configure the function, run the **dot1x unicast-trigger** command.

Item	Description
Trigger dhcp-bind	Whether the device is enabled to automatically generate DHCP snooping binding entries for users with static IP addresses: ● Enable ● Disable To configure the function, run the **dot1x trigger dhcp-binding** command.
Handshake	Whether handshake with online 802.1X authentication users is enabled: ● Enable ● Disable
Handshake packet-type	Type of 802.1X authentication handshake packets: ● request-identity ● srp-sha1-part2
Max retry value	Maximum number of attempts to send authentication requests to 802.1X users. To configure the maximum value, run the **dot1x retry** command.
Reauthen Period	Re-authentication interval for online 802.1X users. To configure the re-authentication interval, run the **dot1x timer** command.
Client Timeout	Authentication timeout period for 802.1X clients. To configure the authentication timeout period, run the **dot1x timer** command.
Handshake Period	Interval at which the device handshakes with an 802.1X client on a non-Eth-Trunk interface. To configure the interval, run the **dot1x timer** command.
Eth-trunk handshake period	Interval at which the device handshakes with an 802.1X client on an Eth-Trunk. To configure the interval, run the **dot1x timer** command.

Item	Description
Dot1x no-response authorize	Whether the function of not responding to the EAPoL-Start packets sent by clients when the AAA server is Down is enabled: • Enable • Disable To configure the function, run the **dot1x no-response authorize authen-server-down** command.
Dot1x eap-success response	Enable the device to respond to EAP-Success messages when 802.1X authentication fails. • Enable • Disable To configure the function, run the **dot1x authentication-reject response eap-success** command.
Bound authentication profile	Authentication profile to which the 802.1X access profile is bound. To configure the authentication profile, run the **dot1x-access-profile** command.

13.5.99 display dot1x-client-profile configuration

Function

The **display dot1x-client-profile configuration** command displays the configuration of an 802.1X client profile.

NOTE

Only the following models support this command: S5735-L-I, S5735-L1, S5735S-L1, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S.

Format

display dot1x-client-profile configuration [**name** *client-profile-name*]

Parameters

Parameter	Description	Value
name *client-profile-name*	Displays the configuration of an 802.1X client profile with a specified name. If **name** *client-profile-name* is not specified, all 802.1X client profiles configured on the device are displayed. If **name** *client-profile-name* is specified, the detailed configuration of the specified 802.1X client profile is displayed.	The value must be the name of an existing 802.1X client profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an 802.1X client profile, you can run this command to check whether the configuration is correct.

Example

Display all 802.1X client profiles configured on the device.

```
<HUAWEI> display dot1x-client-profile configuration
-------------------------------------------------------------------------------
  ID       Dot1x-client-profile name
-------------------------------------------------------------------------------
   0       dot1x_client_profile_1
   1       dot1x_client_profile_2
-------------------------------------------------------------------------------
```

Table 13-62 Description of the **display dot1x-client-profile configuration** command output

Item	Description
ID	ID of an 802.1X client profile.
Dot1x-client-profile name	Name of an 802.1X client profile.

Display the configuration of the 802.1X client profile **d1**.

```
<HUAWEI> display dot1x-client-profile configuration name d1
  Profile name                : d1
  EAP Method                   : PEAP
  EAP username                 : example
  EAP password                 : ******
  PKI realm name               : -
```

Table 13-63 Description of the **display dot1x-client-profile configuration name** command output

Item	Description
Profile name	Name of an 802.1X client profile.
EAP Method	Access mode of the 802.1X client.
EAP username	User name used by an 802.1X client for authentication.
EAP password	Password used by an 802.1X client for authentication.
PKI realm name	Name of the PKI realm used for TLS authentication.

13.5.100 display dot1x-client statistics

Function

The **display dot1x-client statistics** command displays packet statistics of 802.1X clients.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dot1x-client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays packet statistics of the 802.1X client on a specified interface. If this parameter is not specified, packet statistics of 802.1X clients on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view packet statistics of 802.1X clients.

Example

Display packet statistics of 802.1X clients.

```
<HUAWEI> display dot1x-client statistics
  Dot1x-client message statistics on interface GigabitEthernet0/0/1 :
  EAPOL Packets: TX     : 0         RX     : 68
  Dot1x-client message statistics on interface GigabitEthernet0/0/2 :
  EAPOL Packets: TX     : 57        RX     : 67
```

Table 13-64 Description of the **display dot1x-client statistics** command output

Item	Description
Dot1x-client statistics on interface *interface-type interface-number*	Packet statistics of 802.1X clients on an interface.
EAPOL Packets	EAPoL packet statistics.
TX	Number of sent packets.
RX	Number of received packets.

Display packet statistics of 802.1X clients on a specified interface.

```
<HUAWEI> display dot1x-client statistics interface gigabitEthernet 0/0/1
  EAPOL Packets: TX     : 8214      RX     : 9703
  Send      EAPOL Start Packets           : 4714
```



```
        EAPOL Logoff Packets           : 15
        EAPOL Response/Identity Packets : 1415
        EAPOL Response/Challenge Packets: 3954
Received  EAPOL Request/Identity Packets  : 2322
        EAPOL Request/Challenge Packets : 3954
        EAPOL Success Packets          : 35
      EAPOL Failure Packets          : 1508
```

Table 13-65 Description of the **display dot1x-client statistics interface** command output

Item	Description
Sent	Number of sent packets of the following types: • EAPOL Start Packets • EAPOL Logoff Packets • EAPOL Response/Identity Packets • EAPOL Response/Challenge Packets
Received	Number of received packets of the following types: • EAPOL Request/Identity Packets • EAPOL Request/Challenge Packets • EAPOL Success Packets • EAPOL Failure Packets

13.5.101 display dot1x-client status

Function

The **display dot1x-client status** command displays status information of 802.1X clients.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dot1x-client status [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays status information of 802.1X clients on a specified interface. If this parameter is not specified, the status information of 802.1X clients on all interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view status information of 802.1X clients.

Example

Display status information of 802.1X clients.

```
<HUAWEI> display dot1x-client status
  Dot1x-client status on interface GigabitEthernet0/0/1 :
  Access-status: Success
  Access-Time  : 2019/4/19 15:41:35
```

Table 13-66 Description of the **display dot1x-client status** command output

Item	Description
Dot1x-client status on interface *interface-type interface-number*	Status of the 802.1X client on an interface.
Access-status	Access status: • Init: The 802.1X client is in initialization state. • Success: The 802.1X client accesses the network successfully. • Failure: The 802.1X client fails to access the network. • Authenticating: The 802.1X client is being authenticated.

Item	Description
Access-Time	Access time.

13.5.102 display dot1x quiet-user

Function

The **display dot1x quiet-user** command displays information about 802.1X authentication users who are quieted.

Format

display dot1x quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all 802.1X authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a quiet 802.1X authentication user with a specified MAC address.	The value is in H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about 802.1X authentication users who are quieted.

Example

Display information about all 802.1X authentication users who are quieted.

```
<HUAWEI> display dot1x quiet-user all
--------------------------------------------------------------------------------
MacAddress              User Status             Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
```



```
00e0-fc02-0003              Block                 50
------------------------------------------------------------------------------
Total: 1  Printed: 1  Block: 1  Active: 0
```

Table 13-67 Description of the **display dot1x quiet-user all** command output

Item	Description
MacAddress	MAC address of an 802.1X authentication user who is quieted.
User Status	User status: • Block: The user is in silent state. • Active: The user is not in silent state.
Quiet Remain Time(Sec)	• If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. • If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.

13.5.103 display dns snooping interface enable-list

Function

The **display dns snooping interface enable-list** command displays information about the interfaces enabled with DNS snooping.

NOTE

Only the following switch models support this command:
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dns snooping interface enable-list

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view information about the interfaces enabled with DNS snooping.

Example

Display information about the interfaces enabled with DNS snooping.

```
<HUAWEI> display dns snooping interface enable-list
-------------------------------------------------------------
 Total count : 1
-------------------------------------------------------------
 Interface Name
 GigabitEthernet0/0/1
-------------------------------------------------------------
```

Table 13-68 Description of the **display dns snooping interface enable-list** command output

Item	Description
Total count	Number of interfaces enabled with DNS snooping.
Interface Name	Name of an interface.

13.5.104 display dns snooping dn-ip-cache

Function

The **display dns snooping dn-ip-cache** command displays information about DNS snooping IP address and domain name entries.

NOTE

Only the following switch models support this command:
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dns snooping dn-ip-cache

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view information about DNS snooping IP address and domain name entries.

Example

Display information about DNS snooping IP address and domain name entries.

```
<HUAWEI> display dns snooping dn-ip-cache
--------------------------------------------------------------------------------
 Total count    : 1
 TTL delay-time : 22    minute
--------------------------------------------------------------------------------
 IP-address           TTL(minute)  Domain Name
  10.1.1.2            2400         www.example.com
--------------------------------------------------------------------------------
```

Table 13-69 Description of the **display dns snooping dn-ip-cache** command output

Item	Description
Total count	Total number of DNS snooping IP address and domain name entries.
TTL delay-time	Delay in aging DNS snooping IP address and domain name entries, in minutes.
IP-address	IP address obtained through domain name resolution.
TTL(minute)	Time to live (TTL) of IP address and domain name entries, in minutes. **NOTE** The maximum value is 17938897.
Domain Name	Domain name.

13.5.105 display dns snooping dn-rule-list

Function

The **display dns snooping dn-rule-list** command displays information about DNS snooping domain name rule entries.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dns snooping dn-rule-list

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view information about DNS snooping domain name rule entries.

Example

Display information about DNS snooping domain name rule entries.

```
<HUAWEI> display dns snooping dn-rule-list
--------------------------------------------------------------------------------
 Total count : 1
--------------------------------------------------------------------------------
 Index    Priority      Domain Name
   1         11         example.com
--------------------------------------------------------------------------------
```

Table 13-70 Description of the **display dns snooping dn-rule-list** command output

Item	Description
Total count	Total number of DNS snooping domain name rule entries.
Index	Index.
Priority	Priority of a domain name.
Domain Name	Domain name.

13.5.106 display free-rule

Function

The **display free-rule** command displays whether an authentication-free rule defined by ACL is delivered.

Format

display free-rule

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display free-rule** command to view the delivery status of an authentication-free rule defined by ACL.

Example

Display whether an authentication-free rule defined by ACL is delivered.

```
<HUAWEI> display free-rule
-------------------------------------------------------------------------------
  Slot-ID                 Acl-ID                  Status
-------------------------------------------------------------------------------
    0                     6000                    SUCCESS
-------------------------------------------------------------------------------
Total 1 free-rule(s)
```

Table 13-71 Description of the **display free-rule** command output

Item	Description
Slot-ID	Slot ID.
Acl-ID	ACL number.
Status	Whether an authentication-free rule defined by ACL is successfully delivered to a slot.

13.5.107 display free-rule-template configuration

Function

The **display free-rule-template configuration** command displays the configuration of an authentication-free rule profile.

Format

display free-rule-template configuration [**name** *free-rule-name*]

Parameters

Parameter	Description	Value
name *free-rule-name*	Displays the configuration of an authentication-free rule profile with a specified name. If **name** *free-rule-name* is not specified, the device displays all the authentication-free rule profiles configured on the device. If **name** *free-rule-name* is specified, the device displays the configuration of a specified authentication-free rule profile.	The value must be the name of an existing authentication-free rule profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an authentication-free rule profile, you can run this command to check whether the configuration is correct.

Example

Display all the authentication-free rule profiles configured on the device.

```
<HUAWEI> display free-rule-template configuration
------------------------------------------------------------------------------
ID          Free-rule-template Name
------------------------------------------------------------------------------
0           default_free_rule
------------------------------------------------------------------------------
Total: 1 printed: 1.
```

Table 13-72 Description of the **display free-rule-template configuration** command output

Item	Description
ID	ID of an authentication-free rule profile.

Item	Description
Free-rule-template Name	Name of an authentication-free rule profile.

13.5.108 display mac-address authen

Function

The **display mac-address authen** command displays the current authen MAC address entries in the system.

Format

display mac-address authen [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MAC address authentication or 802.1X authentication is configured successfully, the administrator can run this command to check the existing authen MAC address entries on the device. The administrator can check information about user access based on these MAC address entries to locate user access faults. The **authen** entry is generated after a user passes MAC address authentication or 802.1X authentication.

Precautions

If there are a lot of **authen** MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all authen MAC address entries in the system.

```
<HUAWEI> display mac-address authen
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                  Learned-From        Type
--------------------------------------------------------------------------------
xxxx-xxxx-xxxx 3000/-/-                     GE0/0/1             authen
xxxx-xxxx-xxx1 3000/-/-                     GE0/0/1             authen
xxxx-xxxx-xxx2 3000/-/-                     GE0/0/1             authen
--------------------------------------------------------------------------------
Total items displayed = 3
```

Table 13-73 Description of the **display mac-address authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/VSI/BD	VLAN/VSI/BD that the outbound interface belongs to.
Learned-From	Interface on which a MAC address is learned.
Type	Type of a MAC address entry.
Total items displayed	Total number of MAC address entries that match the filter condition.

13.5.109 display mac-address pre-authen

Function

The **display mac-address pre-authen** command displays the current pre-authen MAC address entries in the system.

Format

display mac-address pre-authen [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check the existing MAC address entries of the pre-connection type to obtain access information about pre-connection users and locate faults.

Precautions

If there are a lot of pre-authen MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all pre-authen MAC address entries in the system.

```
<HUAWEI> display mac-address pre-authen
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                  Learned-From       Type
--------------------------------------------------------------------------------
00e0-fc00-0100 3000/-/-                     GE0/0/1            pre-authen
00e0-fc00-0400 3000/-/-                     GE0/0/1            pre-authen
00e0-fc00-0200 3000/-/-                     GE0/0/1            pre-authen
--------------------------------------------------------------------------------
Total items displayed = 3
```

Table 13-74 Description of the **display mac-address pre-authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/VSI/BD	VLAN/VSI/BD that the interface belongs to.
Learned-From	Interface on which a MAC address of a user to be authenticated is learned.
Type	Type of a MAC address entry.
Total items displayed	Total number of MAC address entries that match the filter condition.

13.5.110 display mac-access-profile configuration

Function

The **display mac-access-profile configuration** command displays the configuration of a MAC access profile.

Format

display mac-access-profile configuration [**name** *access-profile-name*]

Parameters

Parameter	Description	Value
name *access-profile-name*	Displays the configuration of a MAC access profile with a specified name. If **name** *access-profile-name* is not specified, the device displays all the MAC access profiles configured on the device. If **name** *access-profile-name* is specified, the device displays the configuration of a specified MAC access profile.	The value must be the name of an existing MAC access profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a MAC access profile, you can run this command to check whether the configuration is correct.

NOTE

The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is not counted in the configuration specification.

Example

Display all the MAC access profiles configured on the device.

```
<HUAWEI> display mac-access-profile configuration
------------------------------------------------------------------------------
ID          Mac-Access-Profile Name
------------------------------------------------------------------------------
0           mac_access_profile
1           m1
2           m2
3           m3
4           m4
------------------------------------------------------------------------------
Total: 5 printed: 5.
```


Table 13-75 Description of the **display mac-access-profile configuration** command output

Item	Description
ID	MAC access profile ID.
Mac-Access-Profile Name	MAC access profile name.

Display the configuration of the MAC access profile **m1** (the MAC address authentication user configures a password).

```
<HUAWEI> display mac-access-profile configuration name m1
  Profile Name                : m1
  Authentication method       : CHAP
  Username format             : fixed username: a1
  Password type               : cipher
  Re-authen                   : Disable
  Trigger condition           : arp dhcp nd dhcpv6
  Offline dhcp-release        : Disable
  Re-authen dhcp-renew        : Disable
  Trigger dhcp-bind           : Enable
  Reauthen Period             : 1800s
  Bound authentication profile : -
```

Display the configuration of the MAC access profile **m2** (the MAC address authentication user does not configure a password).

```
<HUAWEI> display mac-access-profile configuration name m2
  Profile Name                : m2
  Authentication method       : CHAP
  Username format             : fixed username: a1
  Password                    : not configured
  Re-authen                   : Disable
  Trigger condition           : arp dhcp nd dhcpv6
  Offline dhcp-release        : Disable
  Re-authen dhcp-renew        : Disable
  Trigger dhcp-bind           : Enable
  Reauthen Period             : 1800s
  Bound authentication profile : -
```

Table 13-76 Description of the **display mac-access-profile configuration name** command output

Item	Description
Profile Name	MAC access profile name.
Authentication method	Authentication mode for MAC address authentication. • CHAP • PAP To configure the authentication mode, run the **mac-authen authentication-method** command.

Item	Description
Username format	User name format for MAC address authentication. ● use MAC address without-hyphen as username: A user name is a MAC address that does not contain hyphens (-), for example, 0005e01c02e3. ● use MAC address with-hyphen as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 0005-e01c-02e3. ● use MAC address with-hyphen normal as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-05-e0-1c-02-e3. ● use MAC address without-hyphen upper as username: A user name is a MAC address in the uppercase format that does not contain hyphens (-), for example, 0005E01C02E3. ● use MAC address with-hyphen upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 0005-E01C-02E3. ● use MAC address with-hyphen normal upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-05-E0-1C-02-E3. ● use MAC address with-hyphen colon as username: A user name is a MAC address that contains colons (:) and the colons are inserted between every four digits, for example, 0005:e01c:02e3. ● use MAC address with-hyphen normal colon as username: A user name is a MAC address that contains colons (:) and the colons are inserted between every two digits, for example, 00:05:e0:1c:02:e3.

Item	Description
	• use MAC address with-hyphen colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every four digits, for example, 0005:E01C:02E3. • use MAC address with-hyphen normal colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every two digits, for example, 00:05:E0:1C:02:E3. • fixed username: The user name is fixed. • use option82 as username: The content of the Option 82 field is used as the user name. • not configured: The user name format is not configured. To configure the user name format, run the **mac-authen username** command.
Password type	Password display mode for MAC address authentication. • cipher To configure the password display mode, run the **mac-authen username** command.
password	Password of the MAC address authentication user. This field has the following fixed value: • not configured: indicates that the MAC address authentication user does not configure a password.
Re-authen	Whether re-authentication for online MAC address authentication users is enabled: • Enable: indicates that re-authentication is enabled. • Disable: indicates that re-authentication is disabled. To configure the re-authentication function, run the **mac-authen reauthenticate** command.

Item	Description
Trigger condition	Packet type that can trigger MAC address authentication. To configure the packet type, run the **authentication trigger-condition** command.
Offline dhcp-release	Whether the device is enabled to clear user entries when receiving DHCP release packets from MAC address authentication users. ● Enable ● Disable To configure the function, run the **mac-authen offline dhcp-release** command.
Re-authen dhcp-renew	Whether the device is enabled to re-authenticate MAC address authentication users when receiving DHCP lease renewal packets from the users. ● Enable ● Disable To configure the function, run the **mac-authen reauthenticate dhcp-renew** command.
Trigger dhcp-bind	Whether the device is enabled to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-connection phase: ● Enable ● Disable To configure the function, run the **mac-authen trigger dhcp-binding** command.
Reauthen Period	Re-authentication interval for online MAC address authentication users. To configure the re-authentication interval, run the **mac-authen timer reauthenticate-period** command.
Bound authentication profile	Authentication profile to which the MAC access profile is bound. To configure the authentication profile, run the **mac-access-profile** command.

13.5.111 display mac-authen

Function

The **display mac-authen** command displays information about MAC address authentication.

Format

display mac-authen [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> | **configuration**]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays information about MAC address authentication on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. If this parameter is not specified, MAC authentication information of all interfaces is displayed.	-
configuration	Displays the global information about MAC address authentication.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display mac-authen** command to view configuration results of all configuration commands in MAC address authentication. The command output helps you to check whether the MAC address authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

You can locate the fault according to the packet statistics that is displayed using the **display mac-authen** command. When the fault is rectified, run the **reset mac-authen statistics** command to clear the packet statistics. After a period of time, run the **display mac-authen** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

Display the configuration of MAC address authentication.

```
<HUAWEI> display mac-authen
  Quiet period is 60s
  Authentication fail times before quiet is 1
  Maximum users: 16384
  Current users: 1
  Global default domain is default

 GigabitEthernet0/0/1 state: UP.  MAC address authentication is enabled
  MAC access profile is mac_access_profile
  Reauthentication is disabled
  Reauthen Period: 60s
  Maximum users: 16384
  Current users: 1
  Username format: fixed username: gcs
  Password type: cipher
  Authentication Success: 22, Failure: 85
  0 silent mac address(es) found, 0 printed.

 Online user(s) info:
 UserId   MAC/VLAN           AccessTime            UserName
 ------------------------------------------------------------------------------
 37223    00e0-fc12-3456/2003 2014/09/28 15:45:45     gcs
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```


Table 13-77 Description of the **display mac-authen** command output

Item	Description
Quiet period	Quiet period during which the device quiets a user who fails to be authenticated. The default value of the quiet timer is 60 seconds. To configure the quiet period, run the **mac-authen timer quiet-period** command.
Authentication fail times before quiet	Maximum number of authentication failures before the device quiets a user. To configure the maximum value, run the **mac-authen quiet-times** command.
Maximum users	Maximum number of users allowed on the device. The value varies according to device models.
Current users	Number of online users.
Global default domain	Global default authentication domain. To configure the global default authentication domain, run the **domain** command in the system view.
interface state	Interface status: ● UP: The interface is enabled. ● DOWN: The interface is shut down.
MAC address authentication	Whether MAC address authentication is enabled on the interface. ● enabled ● disabled
MAC access profile	MAC access profile name. To configure the MAC access profile name, run the **mac-access-profile** command in the system view.

Item	Description
Reauthentication	Whether re-authentication for MAC address authentication users is enabled. • enabled • disabled To configure whether re-authentication for MAC address authentication users is enabled, run the **mac-authen reauthenticate** command.
Reauthen Period	Re-authentication interval for online MAC address authentication users. To configure the re-authentication interval, run the **mac-authen timer reauthenticate-period** command.
Current users	Number of current online users on the interface.

Item	Description
Username format	User name format for MAC address authentication. ● use MAC address without-hyphen as username: A user name is a MAC address without hyphens (-), for example, 00e0fc123456. ● use MAC address with-hyphen as username: A user name is a MAC address that contains a hyphen (-) in between every four digits, for example, 00e0-fc12-3456. ● use MAC address with-hyphen normal as username: A user name is a MAC address that contains a hyphen (-) in between every two digits, for example, 00-e0-fc-12-34-56. ● use MAC address without-hyphen upper as username: A user name is a MAC address in uppercase format without hyphens (-), for example, 00E0FC123456. ● use MAC address with-hyphen upper as username: A user name is a MAC address in uppercase format that contains a hyphen (-) in between every four digits, for example, 00E0-FC12-3456. ● use MAC address with-hyphen normal upper as username: A user name is a MAC address in uppercase format that contains a hyphen (-) in between every two digits, for example, 00-E0-FC-12-34-56. ● use MAC address with-hyphen colon as username: A user name is a MAC address that contains colons (:) in between every four digits, for example, 00e0:fc12:3456. ● use MAC address with-hyphen normal colon as username: A user name is a MAC address that contains a colon (:) in between every two digits, for example, 00:e0:fc:12:34:56. ● use MAC address with-hyphen colon upper as username: A user

Item	Description
	name is a MAC address in uppercase format that contains a colon (:) in between every four digits, for example, 00E0:FC12:3456. ● use MAC address with-hyphen normal colon upper as username: A user name is a MAC address in uppercase format that contains a colon (:) in between every two digits, for example, 00:E0:FC:12:34:56. ● fixed username: The user name is fixed. ● use option82 as username: The content of the Option 82 field is used as the user name. ● not configured: The user name format is not configured. To configure the user name format for MAC address authentication, run the **mac-authen username** command.
Password type	Password display mode for MAC address authentication. ● cipher To configure the password display mode for MAC address authentication, run the **mac-authen username** command.
Authentication Success: *m*, Failure: *n*	Numbers of successful authentications (*m*) and failed authentications (*n*) on the interface.
m silent mac address(es) found, *n* printed	Numbers of successful authentications (*m*) and failed authentications (*n*) on the interface.
Online user(s) info	Information about online users: ● UserId: ID of an online user. ● MAC/VLAN: MAC address and VLAN of an online user. ● AccessTime: access time of an online user. ● UserName: name of an online user. ● Total: total number of online users. ● printed: number of displayed online users.

13.5.112 display mac-authen quiet-user

Function

The **display mac-authen quiet-user** command displays information about MAC address authentication users who are quieted.

Format

display mac-authen quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all MAC address authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a specified MAC address authentication user who is quieted.	The value is in the H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about MAC address authentication users who are quieted.

Example

Display information about all MAC address authentication users who are quieted.

```
<HUAWEI> display mac-authen quiet-user all
--------------------------------------------------------------------------------
MacAddress              User Status                 Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
xxxx-xxxx-xxxx          Block                       50
--------------------------------------------------------------------------------
Total: 1  Printed: 1  Block: 1  Active: 0
```


Table 13-78 Description of the **display mac-authen quiet-user all** command output

Item	Description
MacAddress	MAC address of a MAC address authentication user who is quieted.
User status	User status: • Block: The user is in a silent state. • Active: The user is not in a silent state.
Quiet Remain Time(Sec)	• If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. • If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.

13.5.113 display portal

Function

The **display portal** command displays the Portal authentication configuration.

Format

display portal [**interface** *interface-type interface-number* | **configuration**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays Portal authentication information of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, Portal authentication information of all interfaces is displayed.	-
configuration	Displays the global Portal authentication information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display portal** command to view the Portal authentication configuration and check whether the configuration is correct.

Example

Display the Portal authentication configuration.

```
<HUAWEI> display portal
  Portal max-user number:16384
  Quiet function is Enabled
  Different-server is Enabled
  Parameter set:Quiet Period       60s   Quiet-times         3
  Logout packets resend: Resend-times 3  Timeout 5s
  Portal Https Redirect: Enable
  Portal JS Redirect   : Enable
  Portal 302 Redirect  : Enable
  Portal Pass Dns      : Enable

  Vlanif10 protocol status: down, web-auth-server layer2(direct)
<HUAWEI> display portal configuration
  Portal CnaBypass     : Enable
```



```
Portal CnaAdaptive    : Disable
Portal max-user number:16384
Quiet function is Enabled
Different-server is Enabled
Parameter set:Quiet Period       60s   Quiet-times        3
Logout packets resend: Resend-times 3  Timeout 5s
Portal Https Redirect: Enable
```

Table 13-79 Description of the **display portal** command output

Item	Description
Portal CnaBypass	Whether the CNA bypass function for iOS terminals is enabled: ● Enabled ● Disabled To enable the CNA bypass function for iOS terminals, run the **portal captive-bypass enable** command.
Portal CnaAdaptives	Whether the Captive Network Assistant (CNA) adaptive function for iOS terminals is enabled: ● Enabled ● Disabled To enable the Captive Network Assistant (CNA) adaptive function for iOS terminals, run the **portal captive-adaptive enable** command.
Portal max-user number	Maximum number of concurrent Portal authentication users allowed to access the device, the value varies according to device models. To set the maximum number of concurrent Portal authentication users allowed to access the device, run the **portal max-user** command.
Quiet function is Enabled or Quiet function is Disabled	Whether the quiet function in Portal authentication is enabled: ● Enabled ● Disabled To enable the quiet function, run the **portal quiet-period** command.

Item	Description
Different-server is Enabled or Different-server is Disabled	Whether a device is enabled to process user logout requests sent by a Portal server other than the one from which users log in: ● Enabled ● Disabled To configure a device to process user logout requests sent by a Portal server other than the one from which users log in, run the **portal logout different-server enable** command.
Parameter set	Parameter settings of the quiet function in Portal authentication. ● Quiet Period: indicates the quiet period in Portal authentication. To set the quiet period in Portal authentication, run the **portal timer quiet-period** command. ● Quiet-times: indicates the maximum number of authentication failures within 60 seconds before a Portal authentication user enters the quiet state. To set the maximum number of authentication failures, run the **portal quiet-times** command.
Logout packets resend	Configuration of the logout packet re-transmission function for Portal authentication users. ● Resend-times: indicates the number of re-transmission times for Portal authentication user logout packets. ● Timeout: indicates the re-transmission interval of Portal authentication user logout packets. To set the re-transmission interval, run the **portal logout resend timeout** command.
Portal Https Redirect	Whether HTTPS redirection of Portal authentication is enabled: ● Enable ● Disable To enable this function, run the **authentication https-redirect enable** command.

Item	Description
Portal JS Redirect	Whether the function of inserting a JavaScript file during Portal redirection is enabled. ● Enable ● Disable To enable this function, run the **portal redirect js enable** command.
Portal 302 Redirect	Whether redirection based on the status code 302 is enabled for Portal authentication: ● Enable ● Disable To configure this function, run the **portal redirect-302 enable** command.
Portal Pass Dns	Whether the device allows DNS packets to pass through during Portal authentication: ● Enable: The device allows DNS packets to pass through during Portal authentication. ● Disable: The device does not allow DNS packets to pass through during Portal authentication. To configure this function, run the **portal pass dns enable** command.
interface protocol status	Link layer protocol state of the interface and the enabled Portal authentication mode. ● up: indicates that the interface is running properly. ● down: indicates that the interface is disabled. ● web-auth-server layer3: indicates that the authentication mode is set to Layer 3 Portal authentication on a specified interface. ● web-auth-server layer2(direct): indicates that the authentication mode is set to Layer 2 Portal authentication on a specified interface.

13.5.114 display portal https-redirect blacklist

Function

The **display portal https-redirect blacklist** command displays IPv4 addresses in the HTTPS redirection blacklist.

The **display portal https-redirect ipv6 blacklist** command displays IPv6 addresses in the HTTPS redirection blacklist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display portal https-redirect blacklist

display portal https-redirect ipv6 blacklist

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the addresses in the HTTPS redirection blacklist are correct.

Example

Display IPv4 addresses in the HTTPS redirection blacklist.

```
<HUAWEI> display portal https-redirect blacklist
---------------------------------------
IP Address       Aging Time
---------------------------------------
 10.1.1.1        2018-06-26 21:01:59
---------------------------------------
 Total:1   Print:1
```

Display IPv6 addresses in the HTTPS redirection blacklist.

```
<HUAWEI> display portal https-redirect ipv6 blacklist
-------------------------------------------------------------
IPv6 Address                        Aging Time
```



```
------------------------------------------------------------------
FC00::1                         2019-02-23 09:47:05
------------------------------------------------------------------
Total:1    Print:1
```

Table 13-80 Description of the **display portal https-redirect blacklist** command output

Item	Description
IP Address/IPv6 Address	IPv4/IPv6 addresses in the blacklist, which is configured using the **portal https-redirect blacklist** command or is added after the condition specified by the **portal https-redirect blacklist packet-rate** or **portal https-redirect blacklist retry-times interval** command is met.
Aging Time	Time when an address in the blacklist is aged out (that is, time when an address is removed from the blacklist). You can run the **portal https-redirect blacklist aging-time** command to configure the aging time of addresses in the blacklist.
Total:*m* Print:*n*	Total number of addresses in the blacklist, and number of addresses displayed.

13.5.115 display portal https-redirect whitelist

Function

The **display portal https-redirect whitelist** command displays IPv4 addresses in the HTTPS redirection whitelist.

The **display portal https-redirect ipv6 whitelist** command displays IPv6 addresses in the HTTPS redirection whitelist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display portal https-redirect whitelist

display portal https-redirect ipv6 whitelist

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the addresses in the HTTPS redirection whitelist are correct.

Example

Display IPv4 addresses in the HTTPS redirection whitelist.

```
<HUAWEI> display portal https-redirect whitelist
IP Address:
-------------------------------
 10.1.2.1
-------------------------------
 Total:1    Print:1
```

Display IPv6 addresses in the HTTPS redirection whitelist.

```
<HUAWEI> display portal https-redirect ipv6 whitelist
IPv6 Address:
------------------------------------------------------------
FC00::2
------------------------------------------------------------
 Total:1    Print:1
```

Table 13-81 Description of the **display portal https-redirect whitelist** command output

Item	Description
IP Address/IPv6 Address	IPv4/IPv6 addresses in the whitelist, which are configured using the **portal https-redirect whitelist** command.
Total:*m* Print:*n*	Total number of addresses in the whitelist, and number of addresses displayed.

13.5.116 display portal-access-profile configuration

Function

The **display portal-access-profile configuration** command displays the configuration of a Portal access profile.

Format

display portal-access-profile configuration [**name** *access-profile-name*]

Parameters

Parameter	Description	Value
name *access-profile-name*	Displays the configuration of a Portal access profile with a specified name. If **name** *access-profile-name* is not specified, the device displays all the Portal access profiles configured on the device. If **name** *access-profile-name* is specified, the device displays the configuration of a specified Portal access profile.	The value must be the name of an existing Portal access profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a Portal access profile, you can run this command to check whether the configuration is correct.

NOTE

The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is not counted in the configuration specification.

Example

Display all the Portal access profiles configured on the device.

```
<HUAWEI> display portal-access-profile configuration
-------------------------------------------------------------------------------
ID          Portal-access-profile Name
-------------------------------------------------------------------------------
0           portal_access_profile
1           p1
2           p2
-------------------------------------------------------------------------------
Total: 3 printed: 3.
```


Table 13-82 Description of the **display portal-access-profile configuration** command output

Item	Description
ID	Portal access profile ID.
Portal-access-profile Name	Portal access profile name.

Display the configuration of the Portal access profile **p1**.

```
<HUAWEI> display portal-access-profile configuration name p1
  Profile name                    : p1
  Portal timer offline-detect length: 300
  Service-scheme name             : -
  Ucl-group name                  : -
  Re-auth                         : Disable
  Network IP Num                  : 1
  Network IP List                 : 10.1.1.0 255.255.255.0
  Web-auth-server Name            : abc
  Layer                           : Layer two portal
  Bound authentication profile    : p1
```

Table 13-83 Description of the **display portal-access-profile configuration name** command output

Item	Description
Profile name	Portal access profile name.
Portal timer offline-detect length	Offline detection interval for Portal authentication users. To configure the interval, run the **portal timer offline-detect** command.
Service-scheme name	Name of the service scheme based on which the device assigns network access rights to users when the Portal server is Down. To configure the service scheme name, run the **authentication event portal-server-down action authorize** command.
Ucl-group name	Name of the UCL group based on which the device assigns network access rights to users when the Portal server is Down. To configure the UCL group name, run the **authentication event portal-server-down action authorize** command.

Item	Description
Re-auth	Whether the device is enabled to re-authenticate users when the Portal server changes from Down to Up. • Enable • Disable To configure the function, run the **authentication event portal-server-up action re-authen** command.
Network IP Num	Number of source IP address segments for Portal authentication. To configure the number, run the **portal auth-network** command.
Network IP List	Source IP address segment for Portal authentication. To configure the source IP address segment, run the **portal auth-network** command.
Web-auth-server Name	Portal server template bound to the Portal access profile. To configure the Portal server template, run the **web-auth-server** command.
Layer	Portal authentication mode. • Layer two portal: Layer 2 authentication mode. • Layer three portal: Layer 3 authentication mode. To configure the Portal authentication mode, run the **web-auth-server** command.
Bound authentication profile	Authentication profile to which the Portal access profile is bound. To configure the authentication profile, run the **portal-access-profile** command.

13.5.117 display portal quiet-user

Function

The **display portal quiet-user** command displays information about Portal authentication users in quiet state.

Format

display portal quiet-user { **all** | **user-ip** *ip-address* | **server-ip** *ip-address* }

Parameters

Parameter	Description	Value
all	Displays information about all Portal authentication users in quiet state.	-
user-ip *ip-address*	Displays information about the quiet user with the specified IP address.	The value is in dotted decimal notation.
server-ip *ip-address*	Displays information about all the users in quiet state authenticated by the Portal authentication server with a specified IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the quiet timer is enabled, you can run the **display portal quiet-user** command to view information about Portal authentication users who are in quiet state.

Example

Display information about all Portal authentication users in quiet state.

```
<HUAWEI> display portal quiet-user all
Quiet IP information
--------------------------------------------------------------------------------
Quiet ip              User status             Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
192.168.1.1             Active                10
192.168.1.2             Block                 20
--------------------------------------------------------------------------------
Total: 2  Printed: 2  Block: 1   Active: 1
```

Display information about the user in quiet state at 192.168.1.1.

```
<HUAWEI> display portal quiet-user user-ip 192.168.1.1
  Quiet remain seconds: 50
  User Status: Block
```


Table 13-84 Description of the **display portal quiet-user** command output

Item	Description
Quiet IP information	Information about the user in quiet state.
Quiet ip	IP address of the user in quiet state.
User status	User status: • Block: The user is in silent state. • Active: The user is not in silent state. Currently, only users in silent state can be displayed.
Quiet Remain Time(Sec)	• If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. • If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.
Quiet remain seconds	Remaining quiet period of the user in quiet state, in seconds.

13.5.118 display portal url-encode configuration

Function

The **display portal url-encode configuration** command displays the configuration of URL encoding and decoding.

Format

display portal url-encode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring URL encoding and decoding, you can run the **display portal url-encode configuration** command to check the configuration.

Example

Display the configuration of URL encoding and decoding.

```
<HUAWEI> display portal url-encode configuration
  Portal URL Encode : Disable
```

Table 13-85 Description of the **display portal url-encode configuration** command output

Item	Description
Portal URL Encode	Whether URL encoding and decoding are enabled: • Disable • Enable To configure the function, run the **portal url-encode enable** command.

13.5.119 display portal user-logout

Function

The **display portal user-logout** command displays temporary logout entries of Portal authentication users.

Format

display portal user-logout [**ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Displays temporary logout entries of the Portal authentication user with a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays temporary logout entries of the Portal authentication user with a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a Portal authentication user goes offline, the device sends an offline request packet to the Portal server. If the device does not receive an ACK packet from the Portal server, it records a temporary logout entry of the user. You can run the **display portal user-logout** command to check temporary logout entries of Portal authentication users.

If the parameter **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] is not specified, the temporary logout entries of all Portal authentication users are displayed.

Example

Display the temporary logout entries of all Portal authentication users.

```
<HUAWEI> display portal user-logout
--------------------------------------------------------------
UserIP          Vrf      Resend Times TableID
--------------------------------------------------------------
192.168.111.100 1        3            0
--------------------------------------------------------------
Total: 1, printed: 1
```

Table 13-86 Description of the **display portal user-logout** command output

Item	Description
UserIP	IP address of the Portal authentication user.
Vrf	VPN instance that the Portal authentication user belongs to.
Resend Times	Number of logout packet re-transmission times. To set the number of logout packet re-transmission times, run the **portal logout resend timeout** command.
TableID	Index of the temporary logout entry.
Total: *m*, printed: *n*	Total number of temporary logout entries and number of displayed entries.

13.5.120 display portal-server state

Function

The **display portal-server state** command displays the status of a Portal server.

Format

display portal-server state [**web-auth-server** *server-name*]

Parameters

Parameter	Description	Value
web-auth-server *server-name*	Displays information about the Portal server status configured in the specified Portal server template. If this parameter is not specified, status of all Portal servers is displayed.	The Portal server template name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When Portal server is used for Portal authentication, you can run the **display portal-server state** command to check information about the Portal server status.

Example

Display information about the Portal server status configured in the Portal server template **abc**.

```
<HUAWEI> display portal-server state web-auth-server abc
  Web-auth-server     :    abc
  Total-servers       :    4
  Live-servers        :    1
  Critical-num        :    0
  Status              :    Normal
  Ip-address              Status
  192.168.2.1             UP
  192.168.2.2             DOWN
  192.168.2.3             DOWN
  192.168.2.4             DOWN
```

Table 13-87 Description of the **display portal-server state** command output

Item	Description
Web-auth-server	Name of the Portal server template.
Total-servers	Number of Portal servers configured.
Live-servers	Number of Portal servers in Up state.

Item	Description
Critical-num	Minimum number of Portal servers in Up state. If the number of Portal servers is less than this value, enable the survival function in the corresponding Portal server template view.
Status	Status of the Portal server. The values are as follows: • Normal: indicates that the Portal server is in normal state. When the value of **Live-servers** in the command output is greater than the value of **Critical-num**, **Status** is displayed as **Normal**. If the **server-ip** *server-ip-address* &<1-10> command is not run in the Portal server template view to configure an IP address for the Portal server, **Status** is displayed as **Normal**. • Abnormal: indicates that the Portal server is in abnormal state. When the value of **Live-servers** in the command output is less than or equal to the value of **Critical-num, Status** is displayed as **Abnormal**.
Ip-address	IP address of the Portal server.
Status	Whether the Portal server with the specified IP address is reachable. The values are as follows: • UP: reachable • DOWN: unreachable

13.5.121 display server-detect state

Function

The **display server-detect state** command displays the status of a Portal server.

Format

display server-detect state [**web-auth-server** *server-name*]

Parameters

Parameter	Description	Value
web-auth-server *server-name*	Displays information about the Portal server status configured in the specified Portal server template. If this parameter is not specified, status of all Portal servers is displayed.	The Portal server template name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When Portal server is used for Portal authentication, you can run the **display server-detect state** command to check information about the Portal server status.

You are advised to run the **display portal-server state** command to check information of the Portal server status.

Example

Display information about the Portal server status configured in the Portal server template **abc**.

```
<HUAWEI> display server-detect state web-auth-server abc
  Web-auth-server     :    abc
  Total-servers       :    4
  Live-servers        :    1
  Critical-num        :    0
  Status              :    Normal
  Ip-address              Status
  192.168.2.1             UP
  192.168.2.2             DOWN
  192.168.2.3             DOWN
  192.168.2.4             DOWN
```

Table 13-88 Description of the **display server-detect state** command output

Item	Description
Web-auth-server	Name of the Portal server template.
Total-servers	Number of Portal servers configured.
Live-servers	Number of Portal servers in Up state.

Item	Description
Critical-num	Minimum number of Portal servers in Up state. If the number of Portal servers is less than or equal to this value, enable the survival function in the corresponding Portal server template view.
Status	Status of the Portal server. The values are as follows: ● Normal: indicates that the Portal server is in normal state. When *Live-servers* in the command output is larger than *Critical-num*, *Status* is displayed as **Normal**. If the **server-ip** *server-ip-address* &<1-10> command is not run in the Portal server template view to configure an IP address for the Portal server, *Status* is displayed as **Normal**. ● Abnormal: indicates that the Portal server is in abnormal state. When *Live-servers* in the command output is less than or equal to *Critical-num*, *Status* is displayed as **Abnormal**.
Ip-address	IP address of the Portal server.
Status	Whether the Portal server with the specified IP address is reachable. The values are as follows: ● UP: reachable ● DOWN: unreachable

13.5.122 display static-user

Function

The **display static-user** command displays static user information.

Format

display static-user [**domain-name** *domain-name* | **interface** *interface-type interface-number* | **ip-address** *start-ip-address* [*end-ip-address*] | **vpn-instance** *vpn-instance-name*] * [**detail**]

Parameters

Parameter	Description	Value
domain-name *domain-name*	Displays static user information in a specified domain.	The value must be an existing domain name on the device.
interface *interface-type interface-number*	Displays static user information on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
ip-address *start-ip-address* [*end-ip-address*]	Displays static user information in a specified IP address range.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays static user information in a specified VPN instance.	The value must be an existing VPN instance name on the device.
detail	Displays detailed information about static users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a static user is configured, you can run the **display static-user** command to view the static user information.

Example

Display information about all static users configured.

```
<HUAWEI> display static-user
 Not-update-ip enable status: No
 IP-address      Interface       MAC-address    VPN
--------------------------------------------------------------------------------
 10.1.1.6        GE0/0/1         00e0-fc12-3456 -
 10.1.1.7        GE0/0/1         00e0-fc12-3456 -
```



```
10.1.1.8        GE0/0/1        00e0-fc12-3456 -
10.1.1.10       -              00e0-fc12-3478 -
10.1.1.11       -              00e0-fc12-3478 -
10.1.1.12       -              00e0-fc12-3478 -
------------------------------------------------------------------------------
Total item(s) number= 6, displayed number= 6
 Ip-static-user enable status:
------------------------------------------------------------------------------
Vlanif10 : success
------------------------------------------------------------------------------
Total item(s) number= 1, displayed number= 1
```

Display detailed information about all static users.

```
<HUAWEI> display static-user detail
 Not-update-ip enable status: No
------------------------------------------------------------------------------
  IP address                    : 10.1.1.2
  IP static user                : Yes
  Vpn-instance                    : -
  Domain-name                       : local
  Interface                     : -
  MAC address                     : -
  VLAN                          : 10
  Detect                        : Disable
  Keep-online                     : Disable
------------------------------------------------------------------------------
  IP address                    : 10.1.1.4
  IP static user                : Yes
  Vpn-instance                    : -
  Domain-name                       : -
  Interface                     : -
  MAC address                     : -
  VLAN                          : 10
  Detect                        : Disable
  Keep-online                     : Enable
------------------------------------------------------------------------------
Total item(s) number= 2, displayed number= 2

Ip-static-user enable status:
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Total item(s) number= 0, displayed number= 0
```

Table 13-89 Description of the **display static-user** command output

Item	Description
Not-update-ip enable status	Whether the device is disabled from updating IP addresses of static users: • Yes • No To configure the function, run the **static-user not-update-ip enable** command.
IP-address/IP address	IP address of a static user.
Interface	Interface connected to a static user.
MAC-address/MAC address	MAC address of a static user.
VPN/Vpn-instance	VPN instance to which a static user belongs.

Item	Description
Total item(s) number= *m*, displayed number= *n*	The total number of entries is *m* and the number of displayed entries is *n*.
Ip-static-user enable status	Whether the function of identifying static users through IP addresses is enabled. To configure the function, run the **ip-static-user enable** command.
if-n : success	The function of identifying static users through IP addresses is enabled on interface *if-n*.
IP static user	Whether the user is a static user: ● Yes ● No
Domain-name	Domain to which a static user belongs. To configure the function, run the **static-user** command.
VLAN	VLAN to which a static user belongs. To configure the function, run the **static-user** command.
Detect	Whether the device is enabled to send ARP packets to trigger MAC address authentication for offline static users: ● Enable ● Disable To configure the function, run the **static-user** command.
Keep-online	Whether a static user is kept online, with offline detection not performed. ● Enable ● Disable To configure the function, run the **static-user** command.

13.5.123 display ucl-group all

Function

The **display ucl-group all** command displays information about all UCL groups that are created.

Format

display ucl-group all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After creating UCL groups using the **ucl-group** command, you can run the **display ucl-group all** command to check information about the UCL groups.

Example

Display information about all UCL groups.

```
<HUAWEI> display ucl-group all
ID      UCL group name
------------------------------------------------------------------------------
10      example
------------------------------------------------------------------------------
Total : 1
```

Table 13-90 Description of the **display ucl-group all** command output

Item	Description
ID	Index of a UCL group.
UCL group name	Name of a UCL group.

13.5.124 display ucl-group ip domain

Function

The **display ucl-group ip domain** command displays information about IP addresses and domain names of static UCL groups.

NOTE

This command is supported only on the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI.

Format

display ucl-group ip *ip-address* { *mask-length* | *ip-mask* }

display ucl-group ip { *group-index* | **name** *group-name* | **static** | **local-access-user** | **push** | **escape** | **all** } [**verbose**]

display ucl-group domain domain-name *domain-name*

display ucl-group ip domain-ip [**verbose**]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support domain names in static UCL groups.

Parameters

Parameter	Description	Value
ip-address	Displays information about the static UCL group with a specified IP address.	The value must be the IP address of an existing static UCL group.
mask-length	Specifies the mask length of an IP address.	The value must be the IP address mask length of an existing static UCL group.
ip-mask	Specifies the mask of the IP address.	The value must be the IP address mask of an existing static UCL group.
group-index	Displays information about the static UCL group with a specified index.	The value must be the index of an existing static UCL group.
name *group-name*	Displays information about the static UCL group with a specified name.	The value must be the name of an existing static UCL group.

Parameter	Description	Value
static	Displays information about static UCL groups.	-
local-access-user	Displays information about dynamic UCL groups.	-
push	Displays information about pushed UCL groups.	-
escape	Displays information about escape UCL groups.	-
all	Displays information about all static UCL groups.	-
domain-name *domain-name*	Displays information about the static UCL group with a specified domain name.	The value must be an existing domain name on the device.
domain-ip	Displays information about IP addresses generated based on domain names in UCL groups.	-
verbose	Displays detailed information about static UCL groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view UCL groups' IP addresses that are manually added (using the **ucl-group ip** command) and dynamically generated when users go online and are granted UCL groups. When a user goes online successfully, the device grants a UCL group to the user and adds the user's IP address (with a 32-bit mask) to the UCL group. When the user goes offline or the user's IP address changes, the device deletes the corresponding IP address from the UCL group.

Example

Display IP address information of all UCL groups.

```
<HUAWEI> display ucl-group ip all
L: local-access-user, P: push, S: static, D: domain, E: escape
IP/Mask              ID    UCL group name                Type
------------------------------------------------------------------------------
10.9.9.4/32          1     g1                            S
10.10.0.0/16         2     g2                            S
10.9.9.6/32          1     g1                            L
------------------------------------------------------------------------------
Total : 3       Local-access-user : 1       Push : 0     Static : 2       Domain : 0       Escape : 0
```

Display detailed information about all static UCL groups.

```
<HUAWEI> display ucl-group ip static verbose
------------------------------------------------------------------------------
IP/Mask              : 10.9.9.4/32
UCL group ID         : 1
UCL group name       : g1
Type                 : static
Status on slot 0     : Success
IP/Mask              : 10.10.0.0/16

UCL group ID         : 2
UCL group name       : g2
Type                 : static
Status on slot 0     : Success
------------------------------------------------------------------------------
Total : 2       Local-access-user : 0       Push : 0     Static : 2       Domain : 0       Escape : 0
```

Display domain name information of static UCL groups.

```
<HUAWEI> display ucl-group domain domain-name example.com
Domain-name      : example.com
UCL group ID     : 1
UCL group name   : g1
------------------------------------------------------------
IP               : 10.9.9.10
IP               : 10.9.9.12
------------------------------------------------------------
Total : 2
```

Display information about IP addresses generated based on domain names in all static UCL groups.

```
<HUAWEI> display ucl-group ip domain-ip
L: local-access-user, P: push, S: static, D: domain, E: escape
IP/Mask              ID    UCL group name                Type
```



```
--------------------------------------------------------------------------------
9.9.9.4/32          1     g1                          D
9.9.9.5/32          1     g1                          D
10.10.0.0/16         2     g2                          D
--------------------------------------------------------------------------------
Total : 3  Local-access-user : 0    Push : 0  Static : 0    Domain : 3  Escape : 0
```

Table 13-91 Description of the **display ucl-group ip domain** command output

Item	Description
IP/Mask	IP address and mask of a UCL group.
ID	UCL group index.
UCL group ID	UCL group index.
UCL group name	UCL group name.
Type	UCL group type: • Static: static UCL group • Local-access-user: UCL group to which local users belong • Push: pushed UCL group • Escape: escape UCL group • Domain: domain name
Domain-name	Domain name.
Status on slot *n*	UCL group status in slot *n*.

13.5.125 display url-template

Function

The **display url-template** command displays information about URL templates.

Format

display url-template { **all** | **name** *template-name* }

Parameters

Parameter	Description	Value
all	Displays information about all configured URL templates.	-
name *template-name*	Displays information about the URL template with a specified name.	The value must be the name of an existing URL template.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a URL template is configured, you can run the **display url-template** command to view information about the URL template.

Example

Display information about all configured URL templates.

```
<HUAWEI> display url-template all
-------------------------------------------------------------------------------
 Name                        URL     Start  Assignment  Isolate        Index
                           Number  Mark   Mark        Mark
-------------------------------------------------------------------------------
 test                        0      ?     =          &              0
 test2                       0      ?     =          &              1
-------------------------------------------------------------------------------
 Total 2
```

Display information about the URL template **example**.

```
<HUAWEI> display url-template name example
 Name : example
 URL  :
 Start mark      : ?
 Assignment mark : =
 Isolate mark    : &
 Device IP
 Device MAC      :
 AP IP           :
 AP MAC          :
 SSID            :
 User MAC        :
 Redirect URL    :
 User IP address :
 Sysname         :
 User VLAN       :
 Delimiter       :
 Format          :
 Login URL Key   : logiurl
 Login URL       : http:\\example.com
 AP Name         :
 AP Location     :
 AP Group Name   :
 Device IP Value : 10.1.1.1
```

Table 13-92 Description of the **display url-template** command output

Item	Description
Index	Index of a URL template.
Name	Name of a URL template.
URL Number	Number of URLs.

Item	Description
URL	URL of the Portal server. To configure this parameter, run the **url** command in the URL template view.
Start mark/Start Mark	Start character in the URL. To configure this parameter, run the **parameter** command.
Assignment mark/Assignment Mark	Assignment character in the URL. To configure this parameter, run the **parameter** command.
Isolate mark/Isolate Mark	Delimiter between URLs. To configure this parameter, run the **parameter** command.
Device IP	Name of **device-ip** in the URL. To configure this parameter, run the **url-parameter** command.
Device MAC	Name of **device-mac** in the URL. To configure this parameter, run the **url-parameter** command.
AP IP	Name of **ap-ip** in the URL. To configure this parameter, run the **url-parameter** command.
AP MACUser VLAN	Name of **ap-mac** in the URL. To configure this parameter, run the **url-parameter** command.
SSID	Name of **ssid** in the URL. To configure this parameter, run the **url-parameter** command.
User MAC	Name of **user-mac** in the URL. To configure this parameter, run the **url-parameter** command.
Redirect URL	Name of **redirect-url** in the URL. To configure this parameter, run the **url-parameter** command.
User IP address	Name of **user-ipaddress** in the URL. To configure this parameter, run the **url-parameter** command.
Sysname	Name of **sysname** in the URL. To configure this parameter, run the **url-parameter** command.
User VLAN	Name of **user-vlan** in the URL. To configure this parameter, run the **url-parameter** command.

Item	Description
Delimiter	Delimiter between MAC addresses in the URL. To configure this parameter, run the **url-parameter mac-address format** command.
Format	Format of MAC addresses in the URL. To configure this parameter, run the **url-parameter mac-address format** command.
Login URL Key	Identification keyword for the login URL sent to the Portal server during redirection. To configure this parameter, run the **url-parameter** command.
Login URL	Device login URL. To configure this parameter, run the **url-parameter** command.
AP Name	Name of **ap-name** in the URL. To configure this parameter, run the **url-parameter** command.
AP Location	Name of **ap-location** in the URL. To configure this parameter, run the **url-parameter** command.
AP Group Name	Name of **ap-group-name** in the URL. To configure this parameter, run the **url-parameter** command.
Device IP Value	Value of the redirection parameter **device-ip**. To configure this parameter, run the **url-parameter set** command.
AP IP Value	Value of an AP IP address carried in the redirection URL.

13.5.126 display web-auth-server configuration

Function

The **display web-auth-server configuration** command displays the Portal server configuration.

Format

display web-auth-server configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the Portal server template is configured, the **display web-auth-server configuration** command displays the Portal server configuration.

Example

Display the Portal server configuration.

```
<HUAWEI> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled
  Server-Source         : -
 ------------------------------------------------------------------------------
  Enabled protocol      : https
  Listening port        : 8443
  SSL policy            : default_policy
  Server-Source         : -
------------------------------------------------------------------------------
  Web-auth-server Name : example
  Web-auth-server Index: 0
  IP-address           :
  IPv6 Address         :
  Shared-key           :
  Source-IP            : -
  Port / PortFlag      : 50100 / NO
  Server-Source        : 10.1.1.1
  URL                  : https://192.168.2.10:8443/webauth
  URL Template         :
  URL Template ParaName:
  URL Template IVName  :
  URL Template Key     :
  Redirection          : Enable
  Sync                 : Disable
  Sync Seconds         : 300
  Sync Max-times       : 3
  Detect               : Disable
  Detect Seconds       : 60
  Detect Max-times     : 3
  Detect Critical-num  : 0
  Detect Action        :
  Detect Type          : portal
  VPN Instance         :
  Bound Portal profile :
  Protocol             : http
  Http Get-method      : disable
  Password Encrypt     : none
  Cmd ParseKey         : cmd
  Username ParseKey    : username
  Password ParseKey    : password
  MAC Address ParseKey : macaddress
```



```
IP Address ParseKey  : ipaddress
Initial URL ParseKey : initurl
Login Cmd            : login
Logout Cmd           : logout
Login Success
    Reply Type       : redirect initial URL
    Redirect URL     :
    Message          : LoginSuccess!
Login Fail
    Reply Type       : redirect login URL
    Redirect URL     :
    Message          : LoginFail!
Logout Success
    Reply Type       : message
    Redirect URL     :
    Message          : LogoutSuccess!
Logout Fail
    Reply Type       : message
    Redirect URL     :
    Message          : LogoutFail!
------------------------------------------------------------------------------
1 Web authentication server(s) in total
```

Table 13-93 Description of the **display web-auth-server configuration** command output

Item	Description
Listening port	Listening port for Portal protocol packets. To configure a listening port, run the **web-auth-server listening-port** command.
Portal	Portal protocol version. • version 1, version 2: The device supports both the versions V1.0 and V2.0. • version 2: The device supports the versions V2.0. To configure the Portal protocol version, run the **web-auth-server version** command.
Include reply message	Whether the packets sent from the device to the Portal server contain authentication responses. • enabled • disabled To configure this function, run the **web-auth-server reply-message** command.

Item	Description
Server-Source	Local gateway address used by the device to receive and respond to the packets sent by the Portal server when Portal authentication is enabled. To configure this parameter, run the **web-auth-server server-source (system view)** command.
Enabled protocol	Enabled HTTP or HTTPS protocol. ● http ● https To enable the HTTP or HTTPS protocol, run the **portal web-authen-server** command.
Listening port	HTTP or HTTPS port number. To configure the HTTP or HTTPS port number, run the **portal web-authen-server** command.
SSL policy	SSL policy referenced by the HTTPS protocol. To configure the SSL policy referenced by the HTTPS protocol, run the **portal web-authen-server** command.
Server-Source	Local gateway address used by the device to receive and respond to the packets sent by the user terminals when the Portal interconnection function of the HTTP or HTTPS protocol is enabled. To configure this parameter, run the **portal web-authen-server server-source** command.
Web-auth-server Name	Name of the Portal server template. To configure the Portal server template name, run the **web-auth-server (system view)** command.
Web-auth-server Index	Index of the Portal server template.
IP-address	IPv4 address of the Portal server. To configure this parameter, run the **server-ip** command in the Portal server template view.

Item	Description
IPv6 Address	IPv6 address of the Portal server. To configure this parameter, run the **server-ip** command in the Portal server template view.
Shared-key	Shared key of the Portal server. To configure this parameter, run the **shared-key** command in the Portal server template view.
Source-IP	IP address used for communication with the Portal server. To configure this parameter, run the **source-ip** command in the Portal server template view.
Port / PortFlag	• Port: indicates the port number of the Portal server. • PortFlag: indicates whether packets are always sent through this port. To configure this parameter, run the **port** command in the Portal server template view.
Server-Source	Local gateway address used by the device to receive and respond to the packets sent by the Portal server when Portal authentication is enabled. To configure this parameter, run the **server-source** command in the Portal server template view.
URL	URL of the Portal server. To configure this parameter, run the **url** command in the Portal server template view.
URL Template	URL template bound to the Portal server template. To configure this parameter, run the **url-template** command in the Portal server template view.
URL Template ParaName	Encrypted URL parameter name. To configure this parameter, run the **url-template** command in the Portal server template view.

Item	Description
URL Template IVName	Initialization vector (IV) used in URL parameter encryption. To configure this parameter, run the **url-template** command in the Portal server template view.
URL Template Key	Key used in URL parameter encryption. To configure this parameter, run the **url-template** command in the Portal server template view.
Redirection	Redirection status of Portal authentication. • Disable: Redirection of Portal authentication is disabled. • Enable: Redirection of Portal authentication is enabled. To configure this parameter, run the **web-redirection disable** command in the Portal server template view.
Sync	User information synchronization. To enable user information synchronization, run the **user-sync** command.
Sync Seconds	User information synchronization interval. To set the user information synchronization interval, run the **user-sync** command.
Sync Max-times	Maximum number of times that user information synchronization fails. To set the maximum number of times that user information synchronization fails, run the **user-sync** command.
Detect	Portal server detection function. To configure Portal server detection function, run the **server-detect** command.
Detect Seconds	Detection interval of the Portal server. To set the detection interval of the Portal server, run the **server-detect** command.
Detect Max-times	Maximum number of detection failures. To set the maximum number of detection failures, run the **server-detect** command.

Item	Description
Detect Critical-num	Minimum number of Portal servers in Up state. To configure this function, run the **server-detect** command.
Detect Action	Action taken after the number of detection failures exceeds the maximum. ● log: The device sends logs after the number of detection failures exceeds the maximum. ● trap: The device sends traps after the number of detection failures exceeds the maximum. To configure an action taken after the number of detection failures exceeds the maximum, run the **server-detect** command.
Detect Type	Portal server detection mode. ● Portal: Portal-based Portal server detection mode ● HTTP: HTTP-based Portal server detection mode To configure the Portal server detection mode, run the **server-detect type** command.
VPN Instance	VPN instance used in Portal authentication. To configure this parameter, run the **vpn-instance** command in the Portal server template view.
Bound Portal profile	Portal access profile to which the Portal server template is bound. To configure this parameter, run the **web-auth-server** command in the Portal server template view.
Http Get-method	Whether users submit user name and password information to the device in GET mode: ● disable: GET mode is not used. ● enable: GET mode is used. To configure the GET mode, run the **http get-method enable** command.

Item	Description
Protocol	Protocol used in Portal authentication. • portal • http • haca To configure the protocol used in Portal authentication, run the **protocol** command.
Password Encrypt	Password encoding mode: • none: The password is not encoded. • uam: The password is encoded using ASCII characters. To configure the password encoding mode, run the **protocol** command.
Cmd ParseKey	Command identification keyword. To configure the command identification keyword, run the **http-method post** command.
Username ParseKey	User name identification keyword. To configure the user name identification keyword, run the **http-method post** command.
Password ParseKey	User password identification keyword. To configure the user password identification keyword, run the **http-method post** command.
MAC Address ParseKey	User MAC address identification keyword. To configure the user MAC address identification keyword, run the **http-method post** command.
IP Address ParseKey	User IP address identification keyword. To configure the user IP address identification keyword, run the **http-method post** command.
Initial URL ParseKey	User initial login URL identification keyword. To configure the user initial login URL identification keyword, run the **http-method post** command.

Item	Description
Login Cmd	User login identification keyword. To configure the user login identification keyword, run the **http-method post** command.
Logout Cmd	User logout identification keyword. To configure the user logout identification keyword, run the **http-method post** command.
Login Success	User login success.
Reply Type	Redirection response type. ● redirect initial URL: A user is redirected to the initial login URL after successful login. ● redirect login URL: A user is redirected to the login URL after a login failure. ● message: specifies the displayed message. ● redirect URL: A user is redirected to a specified URL. To configure the redirection response type, run the **http-method post** command.
Redirect URL	Redirect URL. To configure the redirect URL, run the **http-method post** command.
Message	Displayed message. To configure the displayed message, run the **http-method post** command.
Login Fail	User login failure.
Logout Success	User logout success.
Logout Fail	User logout failure.

13.5.127 display webmng configuration

Function

The **display webmng configuration** command displays the configuration of the WEBMNG module.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S support this command.

Format

display webmng configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring user management based on HTTP or HTTPS, you can run this command to check the configuration of the WEBMNG module.

Example

Display the configuration of the WEBMNG module.

```
<HUAWEI> display webmng configuration
  Manager Type          : http
  Ssl-policy            : -
  Port                  : 8080
  Acl                   : -
```

Table 13-94 Description of the **display webmng configuration** command output

Item	Description
Manager Type	Management type. • http: user management based on HTTP • https: user management based on HTTPS To configure the management type, run the **remote-access-user manage** command.

Item	Description
Ssl-policy	SSL policy used by the built-in Portal server. To configure the SSL policy, run the **remote-access-user manage** command.
Port	Port number for user management based on HTTP or HTTPS. To configure the port number, run the **remote-access-user manage** command.
Acl	ACL number. You can use an ACL to specify users to be managed. To configure the ACL number, run the **remote-access-user manage** command.

13.5.128 domain mac-authen force

Function

The **domain mac-authen force** command configures a forcible domain for MAC address authentication users.

The **undo domain mac-authen force** command deletes a configured forcible domain for MAC address authentication users.

By default, no forcible domain is configured for MAC address authentication users.

Format

domain *domain-name* **mac-authen force mac-address** *mac-address* **mask** *mask*

undo domain *domain-name* **mac-authen force mac-address** *mac-address*

Parameters

Parameter	Description	Value
domain-name	Specifies the forcible domain name.	The value must be an existing domain name on the device.

Parameter	Description	Value
mac-address *mac-address* **mask** *mask*	Specifies a MAC address range within which the MAC address authentication users use the forcible domain. • **mac-address** *mac-address*: specifies the user MAC address. • **mask** *mask*: specifies the MAC address mask. **NOTE** A maximum of 128 MAC address ranges can be specified.	Both the MAC address and mask are in the H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure a forcible domain for MAC address authentication users within a specified MAC address range in the system view.

Prerequisites

A domain has been created using the **domain** command.

Precautions

The priorities of the forcible domain, domain carried in the user name, and default domain in different views are as follows in descending order: forcible domain with a specified authentication mode in an authentication profile > forcible domain in an authentication profile > authentication domain carried in the user name > default domain with a specified authentication mode in an authentication profile > default domain in an authentication profile > global default domain. Note that a forcible domain specified for MAC address authentication users within a MAC address range has the highest priority and takes precedence over that configured in an authentication profile.

This function takes effect only for users who go online after this function is successfully configured.

Example

In the system view, configure the forcible domain **example** for MAC address authentication users within the MAC address range specified using MAC address 00e0-fc95-7231 and mask FFFF-FFFF-FF00.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain example
[HUAWEI-aaa-domain-example] quit
[HUAWEI-aaa] quit
[HUAWEI] domain example mac-authen force mac-address 00e0-fc95-7231 mask ffff-ffff-ff00
```

13.5.129 dot1x abnormal-track cache-record-num

Function

The **dot1x abnormal-track cache-record-num** command sets the maximum number of EAP packets that can be recorded for abnormal 802.1X authentication.

The **undo dot1x abnormal-track cache-record-num** command restores the default maximum number of EAP packets that can be recorded for abnormal 802.1X authentication.

By default, the device can record a maximum of 20 EAP packets for abnormal 802.1X authentication.

Format

dot1x abnormal-track cache-record-num *cache-record-num*

undo dot1x abnormal-track cache-record-num

Parameters

Parameter	Description	Value
cache-record-num	Specifies the maximum number of EAP packets that can be recorded for abnormal 802.1X authentication.	The value is an integer in the range from 0 to 30. The value 0 indicates that no EAP packet is recorded for abnormal 802.1X authentication.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If 802.1X authentication fails, you need to check the EAP packets to locate the fault. This command allows you to set the maximum number of EAP packets that the device can record for abnormal 802.1X authentication.

Example

Set the maximum number of EAP packets that can be recorded for abnormal 802.1X authentication to 30.

```
<HUAWEI> system-view
[HUAWEI] dot1x abnormal-track cache-record-num 30
```

13.5.130 dot1x authentication-method

Function

The **dot1x authentication-method** command configures an 802.1X authentication mode.

The **undo dot1x authentication-method** command restores the default configuration.

The default 802.1X authentication mode is **eap**, which indicates Extensible Authentication Protocol (EAP) relay authentication.

Format

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

Parameters

Parameter	Description	Value
chap	Specifies EAP termination authentication using the Challenge Handshake Authentication Protocol (CHAP).	-
pap	Specifies EAP termination authentication using the Password Authentication Protocol (PAP).	-
eap	Specifies Extensible Authentication Protocol (EAP) relay authentication.	-

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, users exchange authentication information with the device using EAP packets. The device uses two modes to exchange authentication information with the RADIUS server.

- EAP termination: The device directly parses EAP packets, encapsulates user authentication information into a RADIUS packet, and sends the packet to the RADIUS server for authentication. EAP termination is classified into PAP or CHAP authentication.
  - PAP: The device arranges the MAC address, shared key, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the User-Password attribute.
  - CHAP: The device arranges the CHAP ID, MAC address, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the CHAP-Password and CHAP-Challenge attributes.
- EAP relay (specified by **eap**): The device encapsulates EAP packets into RADIUS packets and sends the RADIUS packets to the RADIUS server. The device does not parse the received EAP packets but encapsulates them into RADIUS packets. This mechanism is called EAP over Radius (EAPoR).

The processing capability of the RADIUS server determines whether EAP termination or EAP relay is used. If the RADIUS server has a higher processing capability and can parse a large number of EAP packets before authentication, the EAP relay mode is recommended. If the RADIUS server has a processing capability not good enough to parse a large number of EAP packets and complete authentication, the EAP termination mode is recommended and the device parses EAP packets for the RADIUS server. When the authentication packet processing method is configured, ensure that the client and server both support this method; otherwise, the users cannot pass authentication.

NOTE

- The EAP relay can be configured for 802.1X users only when RADIUS authentication is used.
- If AAA local authentication is used, the authentication mode for 802.1X users can only be set to EAP termination.
- Because mobile phones do not support EAP termination mode (PAP and CHAP), the 802.1X authentication + local authentication mode cannot be configured for mobile phones. Terminals such as laptop computers support EAP termination mode only after having third-party clients installed.
- If the 802.1X client uses the MD5 encryption mode, the user authentication mode on the device can be set to EAP or CHAP; if the 802.1X client uses the PEAP authentication mode, the authentication mode on the device can be set to EAP.
- In a wireless access scenario, if WPA or WPA2 authentication mode is configured in the security policy profile, 802.1X authentication does not support pre-authentication domain-based authorization.
- If an interface has online 802.1X users and the authentication mode is changed between EAP termination and EAP relay in the 802.1X access profile bound to the interface, the online 802.1X users will be logged out. If the authentication mode is changed between CHAP and PAP in EAP termination mode, the online 802.1X users will not be logged out.

Example

In the 802.1X access profile **d1**, configure the device to use PAP authentication for 802.1X users.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x authentication-method pap
```

13.5.131 dot1x authentication-reject response eap-success

Function

The **dot1x authentication-reject response eap-success** command enables a device to send EAP-Success packets when 802.1X authentication fails.

The **undo dot1x authentication-reject response eap-success** command disables a device from sending EAP-Success packets when 802.1X authentication fails.

By default, the device does not send EAP-Success packets when 802.1X authentication fails.

Format

dot1x authentication-reject response eap-success

undo dot1x authentication-reject response eap-success

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

In MAC address + 802.1X hybrid authentication scenarios, a terminal with a built-in 802.1X authentication client displays a message indicating an 802.1X authentication failure when MAC address authentication succeeds. To prevent the message from being displayed, run the **dot1x authentication-reject response eap-success** command to enable the device to send EAP-Success packets when 802.1X authentication fails.

Example

In the 802.1X access profile **d1**, configure the device to send EAP-Success packets when 802.1X authentication fails.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x authentication-reject response eap-success
```

13.5.132 dot1x eap-notify-packet

Function

The **dot1x eap-notify-packet** command configures the device to send EAP packets with a code number to 802.1X users.

The **undo dot1x eap-notify-packet** command restores the default configuration.

By default, the device does not send EAP packets with a code number to users.

Format

dot1x eap-notify-packet eap-code *code-number* **data-type** *type-number*

undo dot1x eap-notify-packet [**eap-code** *code-number* **data-type** *type-number*]

Parameters

Parameter	Description	Value
eap-code *code-number*	Specifies the code number in EAP packets sent by the device.	The value is an integer that ranges from 5 to 255, the default value is 255.
data-type *type-number*	Specifies the data type in EAP packets sent by the device.	The value is an integer that ranges from 1 to 255, the default value is 255.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a non-Huawei device used as the RADIUS server sends RADIUS packets with attribute 61, EAP packet code number 0xa (hexadecimal notation, 10 in decimal notation), and data type being 0x19 (hexadecimal notation, 25 in decimal notation) to the device, run the **dot1x eap-notify-packet** command on the device so that the device can send EAP packets with code number 0xa and data type 0x19 to users. If the **dot1x eap-notify-packet** command is not executed, the device does not process EAP packets of this type and users are disconnected.

Precautions

The device can only send EAP packets with code number 10 and data type 25.

Example

In the 802.1X access profile **d1**, configure the device to send EAP packets with code number 10 and data type 25 to users.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x eap-notify-packet eap-code 10 data-type 25
```

13.5.133 dot1x-client-profile (AP wired port profile view)

Function

The **dot1x-client-profile** command binds a specified 802.1X client profile to an AP wired port profile.

The **undo dot1x-client-profile** command removes the binding relationship between an 802.1X client profile and an AP wired port profile.

By default, no 802.1X client profile is bound to an AP wired port profile.

NOTE

This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Format

dot1x-client-profile *client-profile-name*

undo dot1x-client-profile

Parameters

Parameter	Description	Value
client-profile-name	Specifies the name of an 802.1X client profile.	The 802.1X client profile must already exist.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an 802.1X client profile is created using the **dot1x-client-profile (system view)** command, the profile takes effect only after being bound to an AP wired port profile.

Precautions

- The 802.1X client profile can be bound only to the upstream wired port of an AP.
- The **eth-trunk** and **dot1x-client-profile (AP wired port profile view)** commands cannot be both configured in the AP wired port profile view.

Example

Create an 802.1X client profile named **dot1x_client_profile1**, bind the profile to the AP wired port profile named **wired**, and apply the AP wired port profile to GE0.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name dot1x_client_profile1
[HUAWEI-dot1x-client-profile-dot1x_client_profile1] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] dot1x-client-profile dot1x_client_profile1
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

13.5.134 dot1x-client-profile (interface view)

Function

The **dot1x-client-profile** command applies an 802.1X client profile to an interface.

The **undo dot1x-client-profile** command cancels applying an 802.1X client profile to an interface.

By default, no 802.1X client profile is applied to an interface.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dot1x-client-profile *client-profile-name*

undo dot1x-client-profile *client-profile-name*

Parameters

Parameter	Description	Value
client-profile-name	Specifies the name of an 802.1X client profile.	The 802.1X client profile must exist.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating an 802.1X client profile using the **dot1x-client-profile** (system view) command, you need to apply the profile to an interface to make it take effect.

Precautions

An 802.1X client profile can be applied only to physical interfaces and Eth-Trunks.

Example

Apply an 802.1X client profile named **dot1x_client_profile1** to an interface.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name dot1x_client_profile1
[HUAWEI-dot1x-client-profile-dot1x_client_profile1] quit
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] dot1x-client-profile dot1x_client_profile1
```


13.5.135 dot1x-client-profile (system view)

Function

The **dot1x-client-profile** command creates an 802.1X client profile and displays the 802.1X client profile view.

The **undo dot1x-client-profile** command deletes an 802.1X client profile.

By default, no 802.1X client profile is created.

NOTE

Only the following models support this command: S5735-L-I, S5735-L1, S5735S-L1, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S.

Format

dot1x-client-profile name *client-profile-name*

undo dot1x-client-profile name *client-profile-name*

Parameters

Parameter	Description	Value
name *client-profile-name*	Specifies the name of an 802.1X client profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following special characters: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses an 802.1X client profile to manage all configurations of the 802.1X client.

Precautions

802.1X client authentication and 802.1X access authentication are mutually exclusive. That is, the two functions cannot be configured simultaneously.

Example

Create the 802.1X client profile **dot1x_client_profile1**.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name dot1x_client_profile1
```

13.5.136 dot1x mc-trigger

Function

The **dot1x mc-trigger** command enables multicast-triggered 802.1X authentication.

The **undo dot1x mc-trigger** command disables multicast-triggered 802.1X authentication.

By default, multicast-triggered 802.1X authentication is enabled.

Format

dot1x mc-trigger

undo dot1x mc-trigger

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a client (for example, the built-in 802.1X client of the Windows operating system) cannot send an EAPOL-Start packet to perform 802.1X authentication, you can enable multicast-triggered 802.1X authentication. After that, the device multicasts an EAP-Request/Identity packet to the client to trigger authentication.

Example

Enable multicast-triggered 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x mc-trigger
```


13.5.137 dot1x mc-trigger port-up-send enable

Function

The **dot1x mc-trigger port-up-send enable** command enables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

The **undo dot1x mc-trigger port-up-send enable** command disables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

By default, the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is disabled.

Format

dot1x mc-trigger port-up-send enable

undo dot1x mc-trigger port-up-send enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the device periodically multicasts EAP-Request/Identity packets to clients so that the clients are triggered to send EAPOL-Start packets for 802.1X authentication. If the device interface connecting to a client changes from Down to Up, the client needs to send EAPOL-Start packets again for 802.1X authentication, which takes a long time. You can run the **dot1x mc-trigger port-up-send enable** command on the device to enable the device interface to multicast EAP-Request/Identity packets to the client to trigger 802.1X authentication immediately after the interface goes Up. This configuration shortens the re-authentication time.

Example

Enable the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

```
<HUAWEI> system-view
[HUAWEI] dot1x mc-trigger port-up-send enable
```


13.5.138 dot1x no-response authorize authen-server-down

Function

The **dot1x no-response authorize authen-server-down** command enables the function of not responding to authentication triggering packets sent by clients when the AAA server is Down.

The **undo dot1x no-response authorize authen-server-down** command disables the function.

By default, the device responds to the authentication triggering packets sent by clients when the AAA server is Up.

Format

dot1x no-response authorize authen-server-down

undo dot1x no-response authorize authen-server-down

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When Cisco AnyConnect is used to perform EAP-FAST authentication, the device responds to the authentication triggering packets sent by the client. If the AAA server is Down, the client enters an abnormal state after receiving response packets from the device and cannot access the network. To prevent this problem, you can run the **dot1x no-response authorize authen-server-down** command to disable the device from responding to the authentication triggering packets sent by the client when the AAA server is Down. In this way, the client can obtain the access permission granted when the AAA server is Down.

802.1X authentication, MAC Address + 802.1X Hybrid Authentication can be triggered in the following scenarios:

- A client sends an EAPoL-Start packet.
- A client sends a DHCP, ARP, DHCPv6, ND, or any other packet.
- The access device sends an EAP-Request/Identity packet.

Precautions

This function is only applicable to MAC and 802.1X mixed authentication scenarios.

This function is effective only for new users who go online after the function is configured.

Only wired users support this function.

For new users having no corresponding entry on the device, this function takes effect only after a forcible domain is configured for the users using the **access-domain** *domain-name* [**dot1x**] **force** command in the authentication profile view.

The function takes effect only after the **authentication event authen-server-down action authorize** command is run in the authentication profile view to configure network access rights granted to users when the authentication server does not respond.

You are advised to run both the **dot1x no-response authorize authen-server-down** and **authentication event authen-server-up action re-authen** commands. This enables the authentication server to re-authenticate users in escape state in a timely manner when the server becomes Up so that these users can access the network.

Example

Enable the function of not responding to the authentication triggering packets sent by clients when the AAA server is Down.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x no-response authorize authen-server-down
```

13.5.139 dot1x port-control

Function

The **dot1x port-control** command sets the authorization state of an interface.

The **undo dot1x port-control** command restores the default authorization state of an interface.

By default, the authorization state of an interface is **auto**.

Format

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** }

undo dot1x port-control

Parameters

Parameter	Description	Value
auto	Indicates that the authorization state of an interface is automatically set. An interface is initially in unauthorized state. In this state, the interface can send and receive authentication packets only, and does not allow users to access network resources. After users are authenticated, the interface transitions to the authorized state and allows the users to access network resources.	-
authorized-force	Sets the authorization state of an interface to forcibly authorized. In this state, the interface does not process authentication packets, and allows users to access network resources without authentication or authorization.	-
unauthorized-force	Sets the authorization state of an interface to forcibly unauthorized. In this state, the interface does not process authentication packets, and denies user access to network resources.	-

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **auto** mode is recommended. Only authenticated users can access network resources. To trust all users on an interface without authentication, configure the **authorized-force** mode. To disable access rights of all users on an interface to ensure security, configure the **unauthorized-force** mode.

Precautions

If 802.1X users on an interface have gone online, changing the authorization state in the 802.1X access profile bound to the interface will make the online 802.1X users go offline.

It is recommended that you set the authorization state of an interface in the early stage of network deployment. When the network is running properly, run the **cut access-user** command to disconnect all users from the interface before changing the authorization state.

Example

Configure the authorization state of an interface as **unauthorized-force** in 802.1X access profile **d1**.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x port-control unauthorized-force
```

13.5.140 dot1x quiet-period

Function

The **dot1x quiet-period** command enables the quiet function for 802.1X authentication users.

The **undo dot1x quiet-period** command disables the quiet function for 802.1X authentication users.

By default, the quiet function is enabled for 802.1X authentication users.

Format

dot1x quiet-period

undo dot1x quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the quiet timer function is enabled, if the number of authentication failures of an 802.1X user exceeds a specified value (set using the **dot1x quiet-times** command) within 60 seconds, the user enters a quiet period. During the quiet period, the device discards the 802.1X authentication request packets from the user. This prevents the impact on the system due to frequent user authentication.

The value of the quiet timer is set using the **dot1x timer quiet-period** command. When the quiet timer expires, the device re-authenticates the user.

Example

Enable the quiet timer.

```
<HUAWEI> system-view
[HUAWEI] dot1x quiet-period
```

13.5.141 dot1x quiet-times

Function

The **dot1x quiet-times** command sets the maximum number of authentication failures within 60 seconds before an 802.1X user enters the quiet state.

The **undo dot1x quiet-times** command restores the default setting.

By default, an 802.1X user enters the quiet state after 10 authentication failures within 60 seconds.

Format

dot1x quiet-times *fail-times*

undo dot1x quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before the 802.1X user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the quiet timer function of the device is enabled using the **dot1x quiet-period** command, if the number of authentication failures of an 802.1X user exceeds the value that is set using the **dot1x quiet-times** command within 60 seconds, the user enters the quiet state. This prevents the impact on the system due to frequent user authentication.

Example

Set the maximum number of authentication failures within 60 seconds before an 802.1X user enters the quiet state to 4.

```
<HUAWEI> system-view
[HUAWEI] dot1x quiet-times 4
```

13.5.142 dot1x reauthenticate mac-address

Function

The **dot1x reauthenticate mac-address** command enables re-authentication for an online 802.1X user with the specified MAC address.

By default, re-authentication is disabled for an online 802.1X user with the specified MAC address.

Format

dot1x reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of an 802.1X user to be re-authenticated.	The value is in H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **dot1x reauthenticate**.

The **dot1x reauthenticate mac-address** and **dot1x reauthenticate** commands re-authenticate online 802.1X users and their difference is as follows:

- The **dot1x reauthenticate mac-address** command configures the device to re-authenticate a specified user for once.
- The **dot1x reauthenticate** command configures the device to re-authenticate all users at intervals.
- The **dot1x reauthenticate mac-address** command does not support re-authentication for 802.1X users in pre-connection state.

Example

Enable re-authentication for an 802.1X user with the MAC address of 00e0-fc01-0005.

```
<HUAWEI> system-view
[HUAWEI] dot1x reauthenticate mac-address 00e0-fc01-0005
```

13.5.143 dot1x reauthenticate

Function

The **dot1x reauthenticate** command configures re-authentication for online 802.1X authentication users.

The **undo dot1x reauthenticate** command restores the default configuration.

By default, re-authentication is not configured for online 802.1X authentication users.

Format

dot1x reauthenticate

undo dot1x reauthenticate

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying the authentication parameters of a user on the authentication server, the administrator must re-authenticate the user in real time to ensure user validity if the user has been online.

After the user goes online, the device saves authentication parameters of the user. After re-authentication is configured for online 802.1X authentication users using

the **dot1x reauthenticate** command in the 802.1X access profile, the device automatically sends the user authentication parameters in the 802.1X access profile to the authentication server at an interval (specified using the **dot1x timer reauthenticate-period** *reauthenticate-period-value* command) for re-authentication. If the user authentication information on the authentication server remains unchanged, the users are kept online. If the information has been changed, the users are disconnected and need to be re-authenticated based on the changed authentication parameters.

Precautions

After re-authentication is configured for online 802.1X authentication users, a large number of 802.1X authentication logs are generated.

This function takes effect only for users who go online after this function is successfully configured.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Example

In the 802.1X access profile **d1**, configure re-authentication for online 802.1X authentication users.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x reauthenticate
```

13.5.144 dot1x receive-packet vlan-ignore

Function

The **dot1x receive-packet vlan-ignore** command enables the VLAN replacement function for EAP packets received by an authentication device.

The **undo dot1x receive-packet vlan-ignore** command disables the VLAN replacement function for EAP packets received by an authentication device.

By default, VLAN replacement is disabled for EAP packets received by an authentication device.

Format

dot1x receive-packet vlan-ignore

undo dot1x receive-packet vlan-ignore

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

If there is a VLANIF interface corresponding to the VLAN allowed by the interconnection interfaces between an 802.1X client and an authentication device, the authentication device generates MAC-VLAN entries corresponding to the VLANIF interface for users in pre-connection state. When the 802.1X client triggers 802.1X authentication again, the authentication device does not return response packets if the VLAN ID carried in the received EAP packet does not match any VLAN information in user entries.

To resolve this problem, you can run this command to enable VLAN replacement for EAP packets received by the authentication device. When receiving an EAP packet with the same MAC address and interface information but a different VLAN ID from that in a user entry, the authentication device replaces the VLAN ID in the packet with that in the user entry, so that 802.1X authentication can proceed.

Example

Enable VLAN replacement for EAP packets received by an authentication device.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x receive-packet vlan-ignore
```

13.5.145 dot1x retry

Function

The **dot1x retry** command configures the number of times an authentication request is retransmitted to an 802.1X user.

The **undo dot1x retry** command restores the default configuration.

By default, the device can retransmit an authentication request to an 802.1X user twice.

Format

dot1x retry *max-retry-value*

undo dot1x retry

Parameters

Parameter	Description	Value
max-retry-value	Specifies the number of times an authentication request is retransmitted to an 802.1X user.	The value is an integer that ranges from 1 to 10.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device does not receive any response from a user within a specified time after sending an authentication request to the user, the device sends the authentication request again. If the authentication request has been sent for the maximum retransmission times and no response is received, the user authentication fails. In this process, the total number of authentication requests sent by the device is *max-retry-value* plus 1.

Precautions

Repeated authentication requests occupy a lot of system resources. When using the **dot1x retry** command, you can set the maximum number of times according to user requirements and device resources. The default value is recommended.

The following table lists the intervals at which the device retransmits different types of packets and related commands.

Packet Type	Interval for Retransmitting Packets	Command
EAP-Request/Identity packet (MAC address bypass authentication is disabled)	*tx-period-value*	**dot1x timer tx-period** *tx-period-value*
EAP-Request/Identity packet (MAC address bypass authentication is enabled)	Integer part of the value calculated using the following formula: *delay-time-value*/(*max-retry-value* + 1)	**dot1x timer mac-bypass-delay** *delay-time-value*
EAP-Request/MD5 Challenge packet	*client-timeout-value*	**dot1x timer client-timeout** *client-timeout-value*

Example

In the 802.1X access profile **d1**, configure the number of times an authentication request can be retransmitted to 802.1X users to 4.


```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x retry 4
```

13.5.146 dot1x send-packet untagged

Function

The **dot1x send-packet untagged** command enables an access device to remove VLAN tags from 802.1X packets to be sent to terminals.

The **undo dot1x send-packet untagged** command disables an access device from removing VLAN tags from 802.1X packets to be sent to terminals.

By default, an access device does not remove VLAN tags from 802.1X packets to be sent to terminals.

Format

dot1x send-packet untagged

undo dot1x send-packet untagged

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some terminals (mainly some models of IP phones) cannot identify the tagged 802.1X packets received from access devices, resulting in 802.1X authentication failures. To resolve this problem, you can run the **dot1x send-packet untagged** command to enable access devices to remove VLAN tags from 802.1X packets to be sent to terminals.

Precautions

- This command is not supported in SVF, policy association, and wireless scenarios.
- If both the **dot1x send-packet untagged** and **authentication control-direction all** commands are configured in the authentication profile view, only the **authentication control-direction all** command takes effect.

Example

In the 802.1X access profile **d1**, enable the access switch to remove VLAN tags from 802.1X packets to be sent to terminals.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x send-packet untagged
```

13.5.147 dot1x send-packet vlan

Function

The **dot1x send-packet vlan** command configures the VLAN ID to be carried in EAP packets sent by an 802.1X client.

The **undo dot1x send-packet vlan** command cancels the configuration.

By default, EAP packets sent by an 802.1X client do not carry VLAN information.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dot1x send-packet vlan *vlan-id*

undo dot1x send-packet vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID to be carried in EAP packets	The value is an integer in the range from 1 to 4094.

Views

802.1X client profile view

Default Level

2: Configuration level

Usage Guidelines

By default, EAP packets sent by a device functioning as an 802.1X client do not carry VLAN information. If the interface of the authentication device connected to the client is a trunk interface and is not configured with the default VLAN, the

interface discards the EAP packets received from the client, causing authentication failures.

You can run this command to configure the EAP packets sent by the 802.1X client to carry the VLAN ID allowed by the connected interface of the authentication device. In this way, the authentication device can properly process the EAP packets sent by the client.

Example

Set the VLAN ID to be carried in EAP packets sent by the 802.1X client to 30.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name d1
[HUAWEI-dot1x-client-profile-d1] dot1x send-packet vlan 30
```

13.5.148 dot1x timer

Function

The **dot1x timer** command configures the parameters of each 802.1X timer.

The **undo dot1x timer** command restores the default settings.

For the default parameter settings of each 802.1X timer, see the parameter description.

Format

dot1x timer { **client-timeout** *client-timeout-value* | **reauthenticate-period** *reauthenticate-period-value* }

undo dot1x timer { **client-timeout** | **reauthenticate-period** }

Parameters

Parameter	Description	Value
client-timeout *client-timeout-value*	Specifies the client authentication timeout interval. You are advised to set this parameter to 30 seconds for wired users. **NOTE** On the network, some terminals may delay in responding to EAP-Request/MD5 Challenge packets sent from the device. If the delay is long, you can increase **client-timeout** *client-timeout-value* so that these terminals can go online. The adjustment rule is as follows: 3 x **client-timeout** *client-timeout-value* > Terminal response delay	The value is an integer in the range from 1 to 120, in seconds. By default, the client authentication timeout interval is 5 seconds.
reauthenticate-period *reauthenticate-period-value*	Specifies the periodic re-authentication period for online 802.1X users.	The value is an integer that ranges from 1 to 65535, in seconds. By default, the periodic re-authentication period is 3600 seconds for online 802.1X users.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, multiple timers are started to implement proper and orderly interactions between access users, access devices, and the authentication server. You can change the values of timers by running the **dot1x timer** command to adjust the interaction process. (The values of some timers cannot be changed.) This command is necessary in special network environments. It is recommended that you retain the default settings of the timers.

This command only sets the values of the timers. To enable the timers, perform corresponding configurations or use default settings.

- The client authentication timeout timer and the interval for sending authentication requests are enabled by default. You can run the **dot1x retry** command to configure the number of retransmissions of authentication request packets when the client authentication times out.
- The re-authentication timer for online 802.1X users is disabled by default. To enable this timer, run the **dot1x reauthenticate** command.
- The online 802.1X user handshake function is disabled by default. You can run the **dot1x handshake** command to enable the online 802.1X user handshake function. The handshake function takes effect only for the wired users.

NOTE

It is recommended that the re-authentication interval be set to the default value. If multiple ACLs need to be delivered during user authorization, you are advised to disable the re-authentication function or set a longer re-authentication interval to improve the device's processing performance.

In remote authentication and authorization, if the re-authentication interval is set to a shorter time, the CPU usage may be higher.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

In the 802.1X access profile **d1**, set the client authentication timeout interval to 90 seconds.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x timer client-timeout 90
```

13.5.149 dot1x timer mac-bypass-delay

Function

The **dot1x timer mac-bypass-delay** command configures the 802.1X authentication timeout timer after which MAC address authentication is performed.

The **undo dot1x timer mac-bypass-delay** command restores the default configuration.

By default, the device performs MAC address authentication if 802.1X authentication is not successful within 30 seconds.

Format

dot1x timer mac-bypass-delay *delay-time-value*

undo dot1x timer mac-bypass-delay

Parameters

Parameter	Description	Value
delay-time-value	Specifies the value of the 802.1X authentication timeout timer after which MAC address authentication is performed.	The value is an integer in the range 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After MAC address bypass authentication is configured, the device performs 802.1X authentication first and starts the timer configured using the **dot1x timer mac-bypass-delay** *delay-time-value* command. If 802.1X authentication is not successful before the timer expires, the device performs MAC address authentication on users. You can run the **dot1x retry** *max-retry-value* command to set the number of times an authentication request is retransmitted to an 802.1X user. The retransmission interval is the integer part of the value calculated using the following formula: *delay-time-value*/(*max-retry-value* + 1)

Example

Configure the device to perform MAC address authentication if 802.1X authentication is not successful within 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer mac-bypass-delay 60
```

13.5.150 dot1x timer quiet-period

Function

The **dot1x timer quiet-period** command configures the quiet period for 802.1X users who fail to be authenticated.

The **undo dot1x timer quiet-period** command restores the default quiet period.

By default, the quiet period is 60 seconds for 802.1X users who fail to be authenticated.

Format

dot1x timer quiet-period *quiet-period-times*

undo dot1x timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-times	Sets the quiet period for 802.1X users who fail to be authenticated.	The value is an integer that ranges from 1 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If an 802.1X authentication user fails to be authenticated consecutively within a short period, the system is affected and a large number of duplicated authentication failure logs are generated.

After the quiet function is enabled using the **dot1x quiet-period** command, if the number of times that an 802.1X user fails to be authenticated within 60s exceeds the upper limit (configured using the **dot1x quiet-times** command), the device discards the user's 802.1X authentication request packets for a period to avoid frequent authentication failures.

Example

Set the quiet period to 100 seconds for 802.1X users who fail to be authenticated.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer quiet-period 100
```

13.5.151 dot1x trigger dhcp-binding

Function

The **dot1x trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-connection phase.

The **undo dot1x trigger dhcp-binding** command restores the default setting.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

Format

dot1x trigger dhcp-binding

undo dot1x trigger dhcp-binding

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through 802.1X authentication, the unauthorized users can obtain the same identities as the authorized users and connect to the network without authentication. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting normal communication between authorized users. To prevent the previous attacks, configure IPSG and DAI. These two functions are implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After the static IP users who pass 802.1X authentication or are at the pre-authentication phase send EAP packets to trigger generation of the user information table, the device automatically generates the DHCP snooping binding table based on the MAC address, IP address, and interface recorded in the table.

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass 802.1X authentication or are at the pre-authentication phase. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.

- In the interface view, run the **arp anti-attack check user-bind enable** command to enable DAI.

Precautions

- To make this function take effect, you must run the **dhcp snooping enable** command on the interface to which the 802.1X access profile is bound to enable the DHCP snooping function on the interface and globally.
- The EAP protocol does not specify a standard attribute to carry IP address information. Therefore, if the EAP request packet sent by a static IP user does not contain an IP address, the IP address information in the DHCP snooping binding table is obtained from the user' first ARP request packet with the same MAC address as the user information table after the user passes authentication. On a network, unauthorized users may forge authorized users' MAC addresses to initiate ARP snooping attacks to devices, and the DHCP snooping binding table generated accordingly may be unreliable. Therefore, the **dot1x trigger dhcp-binding** command is not recommended and you are advised to run the **user-bind static** command to configure the static binding table.
- For users who are assigned IP addresses using DHCP, you do not need to run the **dot1x trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function.
- The IP address in the DHCP snooping binding table is extracted from the ARP request packet (the first ARP request packet sent by the user after the user is authenticated or in the pre-connection state that has the same MAC address in the user information table). If the static IP address of a user is changed, the user needs to be authenticated again.

Example

In the 802.1X access profile **d1**, enable the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x trigger dhcp-binding
```

13.5.152 dot1x timer tx-period

Function

The **dot1x timer tx-period** command sets the interval at which the device sends authentication requests.

The **undo dot1x timer tx-period** command restores the default configuration.

By default, the device sends authentication requests at an interval of 30 seconds.

Format

dot1x timer tx-period *tx-period-value*

undo dot1x timer tx-period

Parameters

Parameter	Description	Value
tx-period-value	Specifies the interval for sending authentication requests.	The value is an integer that ranges from 1 to 120, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device starts the **tx-period** timer in either of the following situations:

- When the client initiates authentication and MAC address bypass authentication is not configured, the device sends a unicast Request/Identity packet to the client and starts the **tx-period** timer. If the client does not respond within the period set by the timer, the device retransmits the authentication request.
- To authenticate the 802.1X clients that cannot initiate authentication, the device periodically sends multicast Request/Identity packets through the 802.1X-enabled interface to the clients at the interval set by the **tx-period** timer.

After MAC address bypass authentication is enabled on a device, the interval at which the device sends unicast Request/Identity packets to clients is determined by *delay-time-value* configured in the **dot1x timer mac-bypass-delay** command and *max-retry-value* configured in the **dot1x retry** command. The retransmission interval is the integer part of the value calculated using the following formula: *delay-time-value*/(*max-retry-value* + 1)

Normally, it is recommended that you retain the default setting of the timer.

Example

Set the interval at which the device sends authentication requests to 90 seconds.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer tx-period 90
```

13.5.153 dot1x unicast-trigger

Function

The **dot1x unicast-trigger** command enables the device to send unicast authentication packets to clients.

The **undo dot1x unicast-trigger** command disables the device from sending unicast authentication packets to clients.

By default, the device is disabled from sending unicast authentication packets to clients.

Format

dot1x unicast-trigger

undo dot1x unicast-trigger

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the pre-connection function is disabled and the **dot1x unicast-trigger** command is run on a device, the device sends a unicast authentication packet to respond to the received ARP , DHCPv6, ND, or DHCP Request packet from a client, which triggers authentication. If the client does not respond within the timeout interval (set by the **dot1x timer client-timeout** *client-timeout-value* command), the device retransmits the unicast packet (the maximum of retransmission times is set by the **dot1x retry** *max-retry-value* command). This function allows users to use the 802.1X client provided by the operating system for authentication, helping quickly deploy an 802.1X network.

After receiving a packet that triggers 802.1X authentication from a client, the device sends a unicast packet to the client. For clients that cannot send packets to trigger 802.1X authentication, configure multicast packets to trigger 802.1X authentication.

Prerequisites

The **undo authentication pre-authen-access enable** command has been run in the system view to disable the pre-connection function globally.

Example

In the 802.1X access profile **d1**, enable 802.1X authentication triggered by unicast packets.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x unicast-trigger
```


13.5.154 dot1x url

Function

The **dot1x url** command configures a redirect URL in 802.1X authentication.

The **undo dot1x url** command cancels the redirect URL configuration in 802.1X authentication.

By default, no redirect URL is configured in 802.1X authentication.

Format

dot1x url *url-string*

undo dot1x url

Parameters

Parameter	Description	Value
url-string	Specifies a redirect URL.	The value is a string of 1 to 247 case-sensitive characters, with spaces and question marks (?) not supported. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the early stage of network deployment, 802.1X client deployment is difficult and requires heavy workload. You can run the **dot1x url** command to set a redirect URL to the web page address for downloading the 802.1X client. When a user attempts to access an IP subnet that requires authentication, the device redirects the user to the redirect URL where the user can download and install the 802.1X client software.

Follow-up Procedure

Run the **free-rule** command to configure the network segment where the redirect URL used in 802.1X authentication belongs or configure the IP address segment of the DNS server as an authentication-free IP subnet.

Precautions

This command applies when users use the 802.1X client software that is not provided by the system.

Wireless users do not support the redirect URL configuration in 802.1X authentication.

The device does not support the triggering of a redirect URL through HTTPS packets.

Example

Set the redirect URL in 802.1X authentication to http://10.1.1.1:8080/download.

```
<HUAWEI> system-view
[HUAWEI] dot1x url http://10.1.1.1:8080/download
```

13.5.155 dot1x-access-profile (authentication profile view)

Function

The **dot1x-access-profile** command binds an authentication profile to an 802.1X access profile.

The **undo dot1x-access-profile** command unbinds an authentication profile from an 802.1X access profile.

By default, an authentication profile is not bound to an 802.1X access profile.

Format

dot1x-access-profile *access-profile-name*

undo dot1x-access-profile

Parameters

Parameter	Description	Value
access-profile-name	Specifies the name of an 802.1X access profile.	The value must be the name of an existing 802.1X access profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After being bound to an 802.1X access profile, the authentication profile is enabled with 802.1X authentication. After the authentication profile is applied to the interface or VAP profile, 802.1X authentication can be performed on online users.

Prerequisites

An 802.1X access profile has been created using the **dot1x-access-profile (system view)** command.

Follow-up Procedure

Run the **authentication-profile** (Interface view or VAP profile view) command to apply the authentication profile to the interface or VAP profile.

Precautions

An authentication profile can be bound to only one 802.1X access profile.

Example

Bind the authentication profile **dot1x_authen_profile1** to the 802.1X access profile **dot1x_access_profile1**.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name dot1x_access_profile1
[HUAWEI-dot1x-access-profile-dot1x_access_profile1] quit
[HUAWEI] authentication-profile name dot1x_authen_profile1
[HUAWEI-authen-profile-dot1x_authen_profile1] dot1x-access-profile dot1x_access_profile1
```

13.5.156 dot1x-access-profile (system view)

Function

The **dot1x-access-profile** command creates an 802.1X access profile and displays the 802.1X access profile view.

The **undo dot1x-access-profile** command deletes an 802.1X access profile.

By default, the device has a built-in 802.1X access profile named dot1x_access_profile.

Format

dot1x-access-profile name *access-profile-name*

undo dot1x-access-profile name *access-profile-name*

Parameters

Parameter	Description	Value
name *access-profile-name*	Specifies the name of an 802.1X access profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses 802.1X access profiles to uniformly manage all 802.1X users access configurations. To perform 802.1X authentication for the users in the interface or VAP profile, bind the authentication profile applied to the interface or VAP profile to an 802.1X access profile.

Follow-up Procedure

Run the **dot1x-access-profile** command in the authentication profile view to bind the authentication profile to an 802.1X access profile.

Precautions

- The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in 802.1X access profile dot1x_access_profile can be modified and applied, but cannot be deleted.
- Before deleting an 802.1X access profile, ensure that this profile is not bound to any authentication profile.
- 802.1X client authentication and 802.1X access authentication are mutually exclusive. The two functions cannot be configured at the same time.

Example

Create the 802.1X access profile named **dot1x_access_profile1**.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name dot1x_access_profile1
```


13.5.157 dns snooping enable

Function

The **dns snooping enable** command enables DNS snooping.

The **undo dns snooping enable** command disables DNS snooping.

By default, DNS snooping is disabled.

NOTE

Only the following switch models support this command:
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dns snooping enable

undo dns snooping enable

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the **ucl-group domain** command is run to configure a domain name of a static UCL group, you also need to run the **dns snooping enable** command to enable the DNS snooping function. After this function is enabled, the device parses the received DNS response packets to obtain IP addresses and generates mappings between the IP addresses and domain names.

Precautions

DNS snooping needs to be applied on the interface connected to the DNS server.

Example

Enable DNS snooping.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dns snooping enable
```


13.5.158 dns snooping server-ip-address

Function

The **dns snooping server-ip-address** command configures the IP address of a DNS server.

The **undo dns snooping server-ip-address** command deletes the configuration of a DNS server IP address.

By default, no DNS server IP address is configured on the device.

NOTE

Only the following switch models support this command:
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dns snooping server-ip-address *server-ip-address*

undo dns snooping server-ip-address *server-ip-address*

Parameters

Parameter	Description	Value
server-ip-address	Specifies the IP address of a DNS server.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After DNS snooping is enabled, the device parses the received DNS response packets to obtain IP addresses and generates mappings between the IP addresses and domain names. To prevent attacks initiated by DNS response packets, you can run the **dns snooping server-ip-address** command to specify the IP address of a DNS server. The device then processes only the DNS response packets with the configured DNS server IP address as the source IP address.

Example

Configure the DNS server IP address 10.1.1.1 on the device.

```
<HUAWEI> system-view
[HUAWEI] dns snooping server-ip-address 10.1.1.1
```


13.5.159 dns snooping ttl delay-time

Function

The **dns snooping ttl delay-time** command configures the delay in aging DNS snooping IP address and domain name entries.

The **undo dns snooping ttl delay-time** command restores the default configuration.

By default, the delay in aging DNS snooping IP address and domain name entries is 5760 minutes.

NOTE

Only the following switch models support this command:
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dns snooping ttl delay-time *delay-time*

undo dns snooping ttl delay-time

Parameters

Parameter	Description	Value
delay-time	Specifies the delay in aging IP address and domain name entries.	The value is an integer in the range from 0 to 43200, in minutes. If the value is set to 0, IP address and domain name entries do not age.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After DNS snooping is enabled using the **dns snooping enable** command, the device parses the received DNS response packets to obtain IP addresses and the aging time, and generates mappings between IP addresses and domain names. By default, the delay in aging IP address and domain name entries is 5760 minutes. You can run the **dns snooping ttl delay-time** command to adjust the delay.

Example

Set the delay in aging DNS snooping IP address and domain name entries to 5700 minutes.


```
<HUAWEI> system-view
[HUAWEI] dns snooping ttl delay-time 5700
```

13.5.160 eap-method

Function

The **eap-method** command sets the authentication mode of the device functioning as an 802.1X client.

The **undo eap-method** command deletes the authentication mode of the device functioning as an 802.1X client.

By default, no authentication mode is configured for the device functioning as an 802.1X client.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

eap-method { **eap-peap username** *username* **password cipher** *password* | **eap-tls username** *username* }

undo eap-method

Parameters

Parameter	Description	Value
eap-peap username *username*	Specifies the user name used for PEAP authentication.	The value is a string of 1 to 127 characters.
password cipher *password*	Specifies the password used for PEAP authentication.	The value is a string of 1 to 127 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.
eap-tls username *username*	Specifies the user name used for TLS authentication.	The value is a string of 1 to 127 characters.

Views

802.1X client profile view

Default Level

2: Configuration level

Usage Guidelines

When the device functions as an 802.1X client, you need to configure the 802.1X authentication mode. Both PEAP authentication and TLS authentication use the EAP relay mode. TLS authentication has higher security than PEAP authentication because:

- In PEAP authentication, the digital certificate is loaded only on the server.
- In TLS authentication, the digital certificate is loaded on both the server and client.

Example

Set the authentication mode of the device functioning as an 802.1X client to PEAP.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name d1
[HUAWEI-dot1x-client-profile-d1] eap-method eap-peap username test password cipher YsHsjx_202206
```

13.5.161 enable (terminal type identification profile view)

Function

The **enable** command enables terminal type identification.

The **undo enable** command disables terminal type identification.

By default, terminal type identification is disabled.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

enable

undo enable

Parameters

None

Views

Terminal type identification profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The terminal type identification profile takes effect immediately when terminal type identification is enabled. The AC analyzes the terminal's MAC address, DHCP Option, and user agent information. If the information matches the rules configured in the profile, the AC identifies the terminal type.

Prerequisite

A terminal type identifier has been configured using the **device-type** command.

Example

Enable terminal type identification.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
[HUAWEI-device-profile-test] device-type test
[HUAWEI-device-profile-test] enable
```

13.5.162 free-rule

Function

The **free-rule** command configures authentication-free rules for NAC authentication users.

The **undo free-rule** command restores the default settings.

By default, no authentication-free rule is configured for NAC authentication users.

Format

Common authentication-free rule:

free-rule *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } [**tcp destination-port** *port* | **udp destination-port** *port*] | **any** } } | **source** { **any** | { **interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* } * } } *

undo free-rule { *rule-id* | **all** }

Authentication-free rule defined by ACL:

free-rule acl { *acl-id* | **acl-name** *acl-name* | **ipv6** *ipv6-acl-id* }

undo free-rule { **acl** { *acl-id* | **acl-name** *acl-name* | **ipv6** *ipv6-acl-id* } | **all** }

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support authentication-free rules defined by IPv6 ACLs.

Parameters

Parameter	Description	Value
rule-id	Specifies the number of an authentication-free rule for NAC authentication users.	The value is an integer. S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: The value range is 0 to 31. S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S : The value range is 0 to 511. S6735-S, S6720-EI, S6720S-EI: The value range is 0 to 255.
destination	Specifies the destination network resource that NAC authentication users can access without authentication.	-
source	Specifies source information for NAC authentication users without authentication.	-
any	Indicates any condition. When **any** is used together with different keywords, the effect of the command is different.	-
interface *interface-type interface-number*	Specifies a source interface in the rule. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** The source interface cannot be a management interface.	-

Parameter	Description	Value
ip *ip-address*	Specifies the source or destination IP address depending on the keyword.	The value is in dotted decimal notation. The configured IP address cannot be 255.255.255.255, all 0s, class D address, class E address, or loopback address. If the IP address is a class A address, the network ID cannot be all 0s.
mask *mask-length*	Specifies the mask length of the source or destination IP address depending on the keyword.	The value is an integer that ranges from 1 to 32.
mask *ip-mask*	Specifies the mask of the source or destination IP address depending on the keyword.	The value is in dotted decimal notation.
tcp destination-port *port*	Specifies a TCP destination port number.	The value is an integer that ranges from 1 to 65535.
udp destination-port *port*	Specifies a UDP destination port number.	The value is an integer that ranges from 1 to 65535.
vlan *vlan-id*	Specifies the VLAN ID of source packets.	The value is an integer that ranges from 1 to 4094.
acl	Specifies an authentication-free rule defined by ACL.	-
acl-id	Specifies the number of an IPv4 ACL.	The value is an integer that ranges from 6000 to 6031.
acl-name *acl-name*	Specifies the name of an IPv4 ACL.	The value must be the name of an existing IPv4 ACL with a number in the range from 6000 to 6031.
ipv6 *ipv6-acl-id*	Specifies the number of an IPv6 ACL.	The value is an integer that ranges from 3000 to 3031.
all	Specifies all rules.	-

Views

Authentication-free rule profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before being authenticated, users need to obtain some network access rights to meet basic network access requirements such as downloading the 802.1X client and updating the antivirus database. After running the **free-rule-template** command in the system view to create an authentication-free rule profile, run the **free-rule** command to configure authentication-free rules in the profile. The users then can obtain some network access rights without authentication.

An authentication-free rule can be a common authentication-free rule or an authentication-free rule defined by an ACL. A common authentication-free rule is determined by parameters such as IP address, MAC address, interface, and VLAN. An authentication-free rule defined by an ACL is determined by the ACL rule (configured using the **rule** command). The destination IP address that users can access without authentication can be specified in both a common authentication-free rule and an authentication-free rule defined by an ACL. In addition, the destination domain name that users can access without authentication can be specified in an authentication-free rule defined by an ACL.

Compared with the authentication-free rule defined by IP address, the one defined by domain name is sometimes simple and convenient. For example, some authentication users who do not have an authentication account must first log in to the official website of a carrier and apply for a member account, or log in using the account of a third party such as Twitter or Facebook. This requires that the users can access specified websites before successful authentication. The domain name of a website is easier to remember than the IP address; therefore, the authentication-free rule defined by ACL can be configured to enable the users to access the domain names of websites without authentication.

Prerequisites

To use the authentication-free rule defined by ACL: An ACL rule has been configured using the **rule** command. This ACL rule can be based on an IP address or a domain name. If the rule is defined by IP address, the **source** and **destination** parameters can be configured; if the rule is defined by domain name, only the **destination** parameter can be configured.

NOTE

If the user ACL is created using a name (specified by *acl-name*), a named ACL has been created and the ACL number (6000-6031) has been specified using the **acl name** *acl-name acl-number* command.

Follow-up Procedure

The domain name specified in an ACL only supports dynamic DNS resolution. Therefore, when you define the authentication-free rule by domain name, configure dynamic DNS resolution on the device. The procedure is as follows:

1. Run the **dns resolve** command in the system view to enable dynamic DNS resolution.
2. Run the **dns server** *ip-address* command in the system view to specify an IP address for the DNS server.

Precautions

Wireless 802.1X authentication does not support this function.

When 802.1X authentication or MAC address authentication is configured on a physical interface, the **free-rule** configuration will not take effect after the **undo authentication pre-authen-access enable** command is configured to disable the pre-connection function.

Pay attention to the following when you use common authentication-free rules:

- When multiple authentication-free rules are configured simultaneously, the system matches the rules one by one.
- In a wireless scenario or an SVF system, only the authentication-free rules with IDs in the range of 0 to 127 on the AP or AS can take effect. On the AC or parent, all configured authentication-free rules take effect.
- In a wireless scenario, the VLAN ID and interface number cannot be specified in authentication-free rules configured on an AP. You are advised to set the authentication-free rule ID to 128 or a larger value when specifying the VLAN ID and interface number. If the ID of an authentication-free rule is less than 128, Portal redirection cannot be performed.
- In an SVF system, interface information in an authentication-free rule is invalid.
- If you specify both the VLAN ID and interface number in an authentication-free rule, the interface must belong to the VLAN. Otherwise, the rule is invalid.
- If the destination port number is configured in an authentication-free rule, fragments cannot match the rule and packets cannot be forwarded.
- No authentication-free rule needs to be configured for DHCP, CAPWAP, ARP, and HTTP packets, because these packets can be processed or forwarded before user authentication. Authentication-free rules must be configured for other protocol packets that need to be forwarded. When the packets need to be processed locally, authentication-free rules need to be configured on only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. Authentication-free rules are not required if the **portal pass dns enable** command has been run to allow DNS packets to pass during Portal authentication. However, this mode is not recommended because the command allows all DNS packets to pass.
  - DHCP packet: If authentication and DHCP are enabled on an interface, authentication can be triggered by DHCP packets and the device acts as the DHCP relay or DHCP server to forward or process DHCP packets. If only authentication is configured on the interface and the DHCP function is not configured, authentication can be triggered by DHCP packets and the device broadcasts the DHCP packets.

  - CAPWAP packet: CAPWAP packets are classified into control packets and data packets. Generally, NAC is still effective for CAPWAP data packets after they are decapsulated, and the authentication-free rule takes effect (except for ARP and DHCP packets that are encapsulated in CAPWAP data packets). CAPWAP control packets are sent to the CPU for processing (such as SVF and wireless scenarios). If authentication is enabled on the physical interface connected to an AP, you need to configure the authentication-free rule to transmit packets from the management VLAN. In this scenario, the server may be overloaded due to multiple times of re-authentication. Therefore, this scenario is not recommended.
  - ARP packet: No authentication-free rule needs to be configured for ARP packets, which can be directly processed or forwarded.
  - HTTP packet: If Portal authentication is enabled on an interface and the destination URL of HTTP packets is not the URL of the Portal server, the device redirects HTTP packets to the Portal server for authentication. If the destination URL matches an authentication-free rule, redirection is not triggered. When both an authentication-free rule and an ACL are configured for authorization, only the authentication-free rule takes effect.

Pay attention to the following when you use authentication-free rules defined by ACLs:

- Authentication-free rules based on domain names are valid for only wireless users. Static UCL group and DNS snooping can be configured for wired users to be authenticated based on domain names.
- When SVF is enabled, authentication-free rules defined by ACL cannot be delivered to an AS.
- An authentication-free rule can be dynamically modified. The authentication-free rule performs the **permit** action no matter whether the action in an ACL rule (configured using the **rule** command) is set to **deny** or **permit**. The ACL rule number ranges from 0 to 127.
- If multiple domain names correspond to the same IP address and one matches the authentication-free rule, other domain names also match the authentication-free rule.

The **free-rule** command configures a rule for specifying the resources accessible to users before authentication. However, this command does not mean that users matching the rule do not need to be authenticated. To free specified users from authentication, run the **access-context profile enable** command to enable the user context identification function, and run the **if-match vlan-id** { *start-vlan-id* [**to** *end-vlan-id*] } &<1-10> command in the user context profile to configure the VLAN ID-based user identification policy. In addition, run the **authentication-mode none** command to enable non-configuration in the authentication scheme bound in the authentication domain of the users.

Example

In the authentication-free rule profile **default_free_rule**, allow all NAC authentication users to access the network with the IP address 10.1.1.1/24 without authentication.


```
<HUAWEI> system-view
[HUAWEI] free-rule-template name default_free_rule
[HUAWEI-free-rule-default_free_rule] free-rule 1 destination ip 10.1.1.1 mask 24 source ip any
```

13.5.163 free-rule-template (authentication profile view)

Function

The **free-rule-template** command binds an authentication-free rule profile to an authentication profile.

The **undo free-rule-template** command unbinds an authentication-free rule profile from an authentication profile.

By default, no authentication-free rule profile is bound to an authentication profile.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

free-rule-template *free-rule-template-name*

undo free-rule-template

Parameters

Parameter	Description	Value
free-rule-template-name	Specifies the name of an authentication-free rule profile.	The value must be the name of an existing authentication-free rule profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before being authenticated, users need to obtain some network access rights to meet basic network access requirements such as downloading the 802.1X client and updating antivirus database. The device uses an authentication-free rule profile to uniformly manage authorization information for authentication-free users. You can define some network access rules in the profile to determine network access rights that can be obtained by authentication-free users. You need to bind a configured authentication-free rule profile to an authentication profile.

Users using the authentication profile then can obtain authentication-free authorization information.

Prerequisites

An authentication-free rule profile has been created using the **free-rule-template** command.

When a large number of APs are online, do not run the **free-rule-template** or **undo free-rule-template** command repeatedly because the device takes time to execute the command. Otherwise, users cannot go online or offline properly in a short period of time.

This command is not supported in AS mode.

For wireless users, the configured authentication-free rule in an authentication-free rule profile takes effect only after the profile is bound to an authentication profile using the **free-rule-template** command in the authentication profile view.

For wired users, an authentication-free rule profile takes effect for all wired users after it is created in the system view. The authentication-free rule profile does not need to be bound to an authentication profile using the **free-rule-template** command in the authentication profile view.

Example

Bind the authentication-free rule profile **default_free_rule** to the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] free-rule-template default_free_rule
```

13.5.164 free-rule-template (system view)

Function

The **free-rule-template** command creates an authentication-free rule profile and displays the authentication-free rule profile view.

By default, the device has a built-in authentication-free rule profile named **default_free_rule**.

Format

free-rule-template name *free-rule-template-name*

Parameters

Parameter	Description	Value
name *free-rule-template-name*	Specifies the name of an authentication-free rule profile.	Currently, the device supports only one authentication-free rule profile, that is, the built-in profile **default_free_rule**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To meet basic network access requirements of users who have not passed authentication, the users need to obtain some network access rights without authentication, for example, download 802.1X client software and update the antivirus database. After creating an authentication-free rule profile using the **free-rule-template** command, you can configure authentication-free rules in the profile to allow the users to access the specified network resources without authentication.

Follow-up Procedure

Run the **free-rule** command in the authentication-free rule profile view to configure authentication-free rules for users.

Precautions

Currently, the device supports only one authentication-free rule profile, that is, the built-in profile **default_free_rule**.

For wireless users, the configured authentication-free rule in an authentication-free rule profile takes effect only after the profile is bound to an authentication profile using the **free-rule-template** command in the authentication profile view.

For wired users, an authentication-free rule profile takes effect for all wired users after it is created in the system view. The authentication-free rule profile does not need to be bound to an authentication profile using the **free-rule-template** command in the authentication profile view.

Example

Display the view of the authentication-free rule profile **default_free_rule**.

```
<HUAWEI> system-view
[HUAWEI] free-rule-template name default_free_rule
[HUAWEI-free-rule-default_free_rule]
```

13.5.165 http parse user-agent enable

Function

The **http parse user-agent enable** command enables the function of extracting User-Agent field information.

The **undo http parse user-agent enable** command disables the function of extracting User-Agent field information.

By default, the function of extracting User-Agent field information is disabled.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

http parse user-agent enable

undo http parse user-agent enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User Agent (UA) is a field in the HTTP packet header. This field carries the following information: operating system used by the device, operating system version, CPU type, browser type, browser version, language used by the browser, and browser plug-in.

If a terminal passes authentication and the UA function is enabled, the AC extracts the UA field from the HTTP Get packet sent from the terminal and sends the extracted information to the terminal type identification module, so that the module can identify the terminal type based on UA information, MAC address, and DHCP Option information.

Precautions

The device can parse the UA field with a maximum of 247 bytes.

This function takes effect only for wireless users.

Example

Enable the UA function.

```
<HUAWEI> system-view
[HUAWEI] http parse user-agent enable
```


13.5.166 http get-method enable

Function

The **http get-method enable** command configures the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

The **undo http get-method enable** command restores the default setting.

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication.

Format

http get-method enable

undo http get-method enable

Parameters

None

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication. You can run the **http get-method enable** command to configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

Precautions

The GET mode has the risk of password disclosure. Therefore, the POST mode is recommended.

This command only applies to scenarios in which HTTP or HTTPS is used for Portal connection establishment.

Example

Configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.


```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] http get-method enable
```

13.5.167 http-method post

Function

The **http-method post** command configures parameters for parsing and replying to POST or GET request packets of the HTTP or HTTPS protocol.

The **undo http-method post** command restores the default configuration.

By default, the system has configured parameters for parsing and replying to POST or GET request packets of the HTTP or HTTPS protocol. For details, see the "Parameters" table.

Format

http-method post { **cmd-key** *cmd-key* [**login** *login-key* | **logout** *logout-key*] * | **init-url-key** *init-url-key* | **login-fail response** { **err-msg** { **authenserve-reply-message** | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] } | **login-success response** { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* } | **logout-fail response** { **msg** *msg* | **redirect-url** *redirect-url* } | **logout-success response** { **msg** *msg* | **redirect-url** *redirect-url* } | **password-key** *password-key* | **user-mac-key** *user-mac-key* | **userip-key** *userip-key* | **username-key** *username-key* } *

undo http-method post { **all** | { **cmd-key** | **init-url-key** | **login-fail** | **login-success** | **logout-fail** | **logout-success** | **password-key** | **user-mac-key** | **userip-key** | **username-key** } * }

Parameters

Parameter	Description	Value
cmd-key *cmd-key*	Specifies the command identification keyword. The default value is **cmd**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
login *login-key*	Specifies the user login identification keyword. The default value is **login**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
logout *logout-key*	Specifies the user logout identification keyword. The default value is **logout**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
init-url-key *init-url-key*	Specifies the identification keyword for the user initial login URL. The default value is **initurl**. The value must be the same as that configured on the Portal server. **NOTE** If this parameter is configured together with other parameters, place this parameter at the end of all parameters.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
login-fail response { **err-msg** { **authenserve-reply-message** | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] }	Specifies the response message upon a user login failure. • **err-msg authenserve-reply-message**: The response message returned by the authentication server is displayed upon a user login failure. • **err-msg msg** *msg*: A specified message is displayed upon a user login failure. • **redirect-login-url**: A user is redirected to the login URL upon a login failure. This mode is used by default. • **redirect-url** *redirect-url*: A user is redirected to a specified URL upon a login failure. • **append-reply-message** *msgkey*: The redirect URL carries the identification keyword for the response message returned by the authentication server.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?). • *msgkey*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
login-success response { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* }	Specifies the response message upon successful user login. • **msg** *msg*: A specified message is displayed upon successful user login. • **redirect-init-url**: A user is redirected to the initial login URL upon successful login. This mode is used by default. • **redirect-url** *redirect-url*: A user is redirected to a specified URL upon successful login.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).
logout-fail response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon a user logout failure. • **msg** *msg*: A specified message is displayed upon a user logout failure. The default value is **LogoutFail!**. • **redirect-url** *redirect-url*: A user is redirected to a specified URL upon a logout failure.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).
logout-success response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon successful user logout. • **msg** *msg*: A specified message is displayed upon successful user logout. The default value is **LogoutSuccess!**. • **redirect-url** *redirect-url*: A user is redirected to a specified URL upon successful logout.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).

Parameter	Description	Value
password-key *password-key*	Specifies the password identification keyword. The default value is **password**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
user-mac-key *user-mac-key*	Specifies the identification keyword for the user MAC address. The default value is **macaddress**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
userip-key *userip-key*	Specifies the identification keyword for the user IP address. The default value is **ipaddress**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
username-key *username-key*	Specifies the user name identification keyword. The default value is **username**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
all	Indicates all parameters.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

When the device uses the HTTP or HTTPS protocol to communicate with the Portal server, a user sends POST or GET request packets (carrying parameters such as the user name and MAC address) to the device as required by the Portal server.

After receiving the POST or GET request packets, the device parses parameters in the packets. If identification keywords of the parameters differ from those configured on the device, the user authentication fails. Therefore, you need to run the **http-method post** command to configure the identification keywords based on the Portal server configuration.

After successful user login or logout, or a user login or logout failure, the device sends the login or logout result to the user based on the **http-method post** command configuration. For example, the device sends the **LogoutSuccess!** message to a user who logs out successfully by default.

Example

Change the command identification keyword to **cmd1** on the device when the command identification keyword in POST request packets is **cmd1** on the connected Portal server.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] http-method post cmd-key cmd1
```

13.5.168 force-push

Function

The **force-push** command enables a pushed URL template or pushed URL.

The **undo force-push** command disables a pushed URL template or pushed URL.

By default, no pushed URL template or pushed URL is enabled.

Format

force-push { **url-template** *template-name* | **url** *url-address* }

undo force-push

Parameters

Parameter	Description	Value
url-template *template-name*	Specifies the name of a pushed URL template.	The value must be the name of an existing URL template.
url *url-address*	Specifies a pushed URL.	The value is a string of 1 to 247 case-sensitive characters, with spaces and question marks (?) not supported. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a user sends an HTTP or HTTPS packet to access a web page for the first time after the user is successfully authenticated, the device forcibly redirects the user to a specified web page. In addition to pushing advertisement pages, the device obtains user terminal information through the HTTP or HTTPS packets sent by users, and applies the information to other services. There are two ways to push web pages:

1. URL: pushes the URL of the specified web page.
2. URL template: pushes a URL template. The URL template must have been created and contains the URL of the pushed web page and URL parameters.

Prerequisites

The URL configured using the **url** command in the URL template view cannot be a redirect URL; otherwise, the **force-push** command does not take effect.

Precautions

For the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the forcible web page push function takes effect only for the first HTTP or HTTPS packet sent from users. If an application that actively sends HTTP or HTTPS packets is installed on a user terminal and the terminal has sent HTTP or HTTPS packets before the user accesses a web page, the user is unaware of the web page push process.

For switches except the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: The forcible web page push function takes effect only when it is used together with a redirect ACL. If a redirect ACL exists in the user table, a web page is forcibly pushed when HTTP or HTTPS packets from users match the redirect ACL rule. Usually, you can configure the RADIUS server to authorize the Huawei extended RADIUS attribute **HW-Redirect-ACL** or **HW-IPv6-Redirect-ACL** to users for redirect ACL implementation, or run the **redirect-acl** command to configure a redirect ACL.

A pushed URL configured in a domain needs to be used together with a redirect ACL or push flag attribute. The redirect ACL has a higher priority than the push flag attribute. By default, a pushed URL configured in a domain carries the push flag attribute. Users will be redirected to the pushed URL when they are successfully authenticated.

When an IPv4 redirect ACL is configured for an IPv6 user or an IPv6 redirect ACL is configured for an IPv4 user, the **Push URL content** field in the **display access-user** command output displays the pushed URL, but the browser of the user cannot redirect to the pushed URL.

Switches except the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support concurrent use of the pushed URL and redirection ACL6 functions. If both functions are configured, the **Push URL content** field in the **display access-user** command output displays the pushed URL; however, the terminal browser cannot be redirected to the pushed URL.

Example

Enable the pushed URL template **abc** in the domain **test**.

```
<HUAWEI> system-view
[HUAWEI] url-template name abc
[HUAWEI-url-template-abc] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] force-push url-template abc
```

13.5.169 if-match vlan-id

Function

The **if-match vlan-id** command configures the VLAN ID-based user identification policy.

The **undo if-match vlan-id** command deletes the VLAN ID-based user identification policy.

By default, no VLAN ID-based user identification policy is configured.

Format

if-match vlan-id { *start-vlan-id* [**to** *end-vlan-id*] } &<1-10>

undo if-match vlan-id { *start-vlan-id* [**to** *end-vlan-id*] } &<1-10>

Parameters

Parameter	Description	Value
start-vlan-id [**to** *end-vlan-id*]	Specifies the start and end user VLAN IDs. The value of *end-vlan-id* must be equal to or greater than that of *start-vlan-id*. If the parameter **to** *end-vlan-id* is not specified, users are classified based on the VLAN ID specified by *start-vlan-id*.	The value of *start-vlan-id* or *end-vlan-id* is an integer that ranges from 1 to 4094.

Views

User context profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On some enterprise networks, VLANs are used to divide the entire network into different areas with various security levels. The administrator requires that a user should obtain different network access rights when the user connects to the network from different areas. In this case, the user context identification function can be enabled on access devices, and a group of VLANs that belong to the same area are added to the same user context profile. The administrator then assigns the mapping network access rights to different user context profiles based on the security level of each area. When a user connects to the network from different areas, the user is added to different user context profiles matching their access VLANs and therefore obtains different network access rights.

Prerequisites

A user context profile has been created using the **access-context profile name** *profile-name* command in the system view.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Example

In the user context profile **p1**, configure the user identification policy of matching users in VLAN 10 to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] access-context profile name p1
[HUAWEI-access-context-p1] if-match vlan-id 10 to 20
```

13.5.170 if-match

Function

The **if-match** command configures the matching mode of terminal type identification rules.

The **undo if-match** command deletes the matching mode of terminal type identification rules.

By default, no matching mode of terminal type identification rules is configured.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

if-match rule *rule-id* [{ **and** | **or** } **rule** *rule-id*] &<1-7>

undo if-match

Parameters

Parameter	Description	Value
rule *rule-id*	Specifies the ID of a terminal type identification rule.	The value is an integer that ranges from 0 to 7.
and	Specifies the matching mode as "and" (that is, a terminal type can be identified only when the terminal information matches all rules configured).	-
or	Specifies the matching mode as "or" (that is, a terminal type can be identified when the terminal information matches any of the rules).	-

Views

Terminal type identification profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **if-match** command allows you to flexibly combine terminal type identification rules.

Prerequisite

The specified terminal type identification rules have been configured using the **rule** command.

Precautions

If the **and** parameter is specified and the terminal information does not match the first rule, the AC sends a matching failure response and stops matching the following rules.

The priority of **and** is higher than that of **or**. For example, you run the **if-match rule 1 or rule 2 and rule 3 or rule 4 and rule 5 or rule 6 and rule 7 or rule 0** command. If the terminal information matches any of the five rule combinations, which are rule 1, rule 2 and rule 3, rule 4 and rule 5, rule 6 and rule 7, and rule 0, the matching operation succeeds.

Example

Specify that terminal information must match terminal type identification rule 1.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
[HUAWEI-device-profile-test] if-match rule 1
```

13.5.171 ip-static-user enable

Function

The **ip-static-user enable** command enables the function of identifying static users through IP addresses.

The **undo ip-static-user enable** command restores the default configuration.

By default, the function of identifying static users through IP addresses is disabled, and the device identifies static users through MAC addresses.

NOTE

This command is supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

ip-static-user enable

undo ip-static-user enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device identifies static users through MAC addresses. However, a terminal may have only one MAC address and multiple IP addresses. The terminal can go online only after its multiple IP addresses pass authentication. If the device identifies terminals through MAC addresses, entry information about a terminal's IP address that is authenticated later overwrites entry information about the terminal's another IP address that is authenticated earlier. As a result, the terminal cannot go online. To resolve this problem, run the **ip-static-user enable** command

to enable the device to identify static users through IP addresses, so that terminals with one MAC address and multiple IP addresses can go online.

Prerequisites

A static user has been configured before this function is enabled.

1. A static user has been configured using the **static-user** *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*] [**ip-user**] [**domain-name** *domain-name* | **interface** *interface-type interface-number* [**detect**] | **mac-address** *mac-address* | **vlan** *vlan-id*] * command.
2. The authentication user name has been configured for the static user using the **static-user username format-include** { **ip-address** | **mac-address** | **system-name** } command.
3. The authentication password has been configured for the static user using the **static-user password cipher** *password* command.

Precautions

- For a terminal with one MAC address and multiple IP addresses, you must configure the terminal as a static user and enable the function of identifying static users through IP addresses so that the terminal can pass authentication and go online. If **ip-user** is not specified when you configure static users, all static users are processed by assuming they have one MAC address and multiple IP addresses. To precisely identify and process static users with one MAC address and multiple IP addresses, specify **ip-user** when configuring these static users.
- The device does not support traffic statistics collection for a terminal with one MAC address and multiple IP addresses.
- This function is supported only for wired users.
- This function takes effect only for new users who go online after the function is configured. After the configuration on an interface is modified, online users on the interface go offline.
- The device supports this function only when the user access mode is **multi-authen**. For details about how to configure the user access mode, see **authentication mode**.
- Static users who are identified through IP addresses will go offline if they fail the authentication. In this case, the **display access-user (all views)** command cannot display any information about these users, including their states: pre-authentication or authentication failure.
- Static users identified through IP addresses do not support MAC address flapping.
- Static users identified through IP addresses do not support permission control during Layer 2 forwarding.
- Static users identified through IP addresses support only IP address-based upstream authorization services (such as UCL-based authorization, isolation between Layer 3 groups, CAR, and priority for upstream traffic), and do not support downstream authorization services (such as CAR, re-marking action, dynamic VLAN-based authorization, and HQoS for downstream traffic).
- In the policy association scenario, if the control point mode is set to **open** using the **authentication control-point open** command, the device does not support the function of identifying static users through IP addresses.

- For a terminal with one MAC address and multiple IP addresses, only ARP packets can trigger authentication. Therefore, ensure that the device can perform authentication triggered by ARP packets; for example, the types of packets that can trigger authentication must include ARP.
- For the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the **ip-static-user enable** and **authentication trigger-condition any-l2-packet** commands are both configured, user authentication cannot be triggered by any Layer 2 packets.
- If user A with multiple IP addresses and one MAC address goes online and then user B with multiple IP addresses and multiple MAC addresses (including user A's MAC address) in a different VLAN from user A also goes online, user A cannot access the network.
- If user A with multiple IP addresses and one MAC address is online and then web user B with the same MAC address is successfully authenticated, the entry of user A is overwritten by that of user B. In this case, user A still has network access rights.

Example

Enable the function of identifying static users through IP addresses in the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] ip-static-user enable
```

13.5.172 link-down offline delay

Function

The **link-down offline delay** command configures the user logout delay when an interface link is faulty.

The **undo link-down offline delay** command restores the default configuration.

By default, the user logout delay is 10 seconds when an interface link is faulty.

Format

link-down offline delay { *delay-value* | **unlimited** }

undo link-down offline delay

Parameters

Parameter	Description	Value
delay-value	Specifies the user logout delay when an interface link is faulty.	The value is an integer that ranges from 0 to 60, in seconds. If the value is 0, users are logged out immediately when an interface link is faulty.

Parameter	Description	Value
unlimited	Indicates that users are not logged out when an interface link is faulty.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a link is faulty, the interface is interrupted and users are directly logged out. To solve this problem, you can configure the user logout delay function. When the interface link is faulty, the users remain online within the delay. In this case, if the link is restored, the users do not need to be re-authenticated. If the users are disconnected after the delay and the link is restored, the users need to be re-authenticated.

Precautions

- This function takes effect only for wired users who go online on Layer 2 physical interfaces that have been configured with NAC authentication.
- To make the function take effect, it is recommended that the configured interval be greater than the time during which the interface is in Up state. If the link frequently flaps within a short period, it is recommended that the interval be set to **unlimited**.

Example

In the authentication profile **p1**, set the user logout delay to 5 seconds when the link is faulty.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] link-down offline delay 5
```

13.5.173 lldp sensor-ap authentication disable

Function

The **lldp sensor-ap authentication disable** command disables an NAC-enabled interface of a switch from performing authentication on Huawei APs identified through LLDP.

The **undo lldp sensor-ap authentication disable** command restores the default configuration.

By default, an NAC-enabled interface on a switch needs to authenticate Huawei APs identified through LLDP.

Format

lldp sensor-ap authentication disable

undo lldp sensor-ap authentication disable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In wired and wireless convergence scenarios, an NAC-enabled interface on a switch authenticates APs and terminals (such as printers and PCs) that go online on this interface. If APs and connected terminals on the live network are secure and do not require NAC authentication, you can run this command to disable authentication on the APs and terminals.

Precautions

- If an AP already has online wireless users, these users will go online after you run the **undo lldp sensor-ap authentication disable** command.
- This command takes effect only when the authentication profile is applied to a Layer 2 interface.
- This function does not take effect in policy association and SVF scenarios.
- This function takes effect only for Huawei APs.
- When an authentication profile configured with this command is bound to an interface, all terminals using this authentication profile can connect to the network without being authenticated.

Example

Disable a switch from performing authentication on Huawei APs identified through LLDP in the view of the authentication profile **authen1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] lldp sensor-ap authentication disable
```


13.5.174 load-file (WLAN view)

Function

The **load-file** command manually loads a certificate file on an AP.

The **undo load-file** command cancels manual certificate file loading on an AP.

By default, no certificate file is manually loaded on an AP.

NOTE

This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Format

load-file { **ap-id** *ap-id* | **ap-group** *ap-group* | **all** }

undo load-file { **ap-id** *ap-id* | **ap-group** *ap-group* | **all** }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Loads a certificate file on an AP with the specified AP ID.	The AP ID must already exist.
ap-group *ap-group*	Loads a certificate file on APs in the specified AP group.	The AP group must already exist.
all	Loads a certificate file on all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When certificate files are configured on an AC, the AC automatically delivers all the certificate files to an AP after the AP goes online. However, if a certificate file is modified or deleted, or a certificate file is added after the AP goes online, the AC cannot automatically deliver the certificate file again. You can run this command to manually deliver the certificate file to the AP.

Precautions

- After the **undo load-file** { **ap-id** *ap-id* | **ap-group** *ap-group* | **all** } command is run, certificate files are no longer delivered to the current AP and subsequent APs. This does not affect the certificate files that have been delivered to APs.
- After the **load-file** { **ap-id** *ap-id* | **ap-group** *ap-group* | **all** } command is run, if a certificate file fails to be loaded on an AP, certificate file re-loading is automatically triggered. By default, a certificate file can be re-loaded three times.
- If a certificate file is being loaded on an AP, the command cannot be run repeatedly.

Example

Manually load certificate files to APs in the AP group named **ap-group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] load-file ap-group ap-group1
```

13.5.175 mac-access-profile (authentication profile view)

Function

The **mac-access-profile** command binds an authentication profile to a MAC access profile.

The **undo mac-access-profile** command unbinds an authentication profile from a MAC access profile.

By default, an authentication profile is not bound to a MAC access profile.

Format

mac-access-profile *access-profile-name*

undo mac-access-profile

Parameters

Parameter	Description	Value
access-profile-name	Specifies the name of a MAC access profile.	The value must be the name of an existing MAC access profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After being bound to a MAC access profile, the authentication profile is enabled with MAC address authentication. After the authentication profile is applied to the interface or VAP profile, MAC address authentication can be performed on online users.

Prerequisites

A MAC access profile has been created using the **mac-access-profile (system view)** command.

Follow-up Procedure

Run the **authentication-profile** command to apply the authentication profile to the interface or VAP profile.

Precautions

An authentication profile can be bound to only one MAC access profile.

Example

Bind the authentication profile **mac_authen_profile1** to the MAC access profile **mac_access_profile**.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] quit
[HUAWEI] authentication-profile name mac_authen_profile1
[HUAWEI-authen-profile-mac_authen_profile1] mac-access-profile mac_access_profile
```

13.5.176 mac-access-profile (system view)

Function

The **mac-access-profile** command creates a MAC access profile and displays the MAC access profile view.

The **undo mac-access-profile** command deletes the MAC access profile.

By default, the device has a built-in MAC access profile named **mac_access_profile**.

Format

mac-access-profile name *access-profile-name*

undo mac-access-profile name *access-profile-name*

Parameters

Parameter	Description	Value
name *access-profile-name*	Specifies the name of a MAC access profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses MAC access profiles to uniformly manage all MAC users access configurations. To perform MAC address authentication for the users in the interface or VAP profile, bind the authentication profile applied to the interface or VAP profile to a MAC access profile.

Follow-up Procedure

Run the **mac-access-profile** command in the authentication profile view to bind the authentication profile to a MAC access profile.

Precautions

- The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in MAC access profile **mac_access_profile** can be modified and applied, but cannot be deleted.
- Before deleting a MAC access profile, ensure that this profile is not bound to any authentication profile.

Example

Create the MAC access profile named **mac_access_profile**.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
```


13.5.177 mac-authen authentication-method

Function

The **mac-authen authentication-method** command configures the authentication mode for MAC address authentication.

The **undo mac-authen authentication-method** command restores the default configuration.

By default, the authentication mode for MAC address authentication is set to PAP.

Format

mac-authen authentication-method { **chap** | **pap** }

undo mac-authen authentication-method

Parameters

Parameter	Description	Value
chap	Indicates the Challenge Handshake Authentication Protocol (CHAP) authentication mode.	-
pap	Indicates the Password Authentication Protocol (PAP) authentication mode.	-

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MAC address authentication, the access device exchanges RADIUS packets with the authentication server. Differences between authentication modes PAP and CHAP are as follows:

- PAP is a two-way handshake authentication protocol. It transmits passwords in plain text format in RADIUS packets.
- CHAP is a three-way handshake authentication protocol. It transmits only user names but not passwords in RADIUS packets.

By default, the authentication mode for MAC address authentication is set to PAP.

Precautions

The authentication server must support CHAP when the authentication mode is set to CHAP.

Example

In the MAC access profile **mac_access_profile**, set the authentication mode for MAC address authentication to CHAP.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] mac-authen authentication-method chap
```

13.5.178 mac-authen offline dhcp-release

Function

The **mac-authen offline dhcp-release** command enables the device to clear user entries when receiving DHCP Release packets from MAC address authentication users.

The **undo mac-authen offline dhcp-release** command restores the default configuration.

By default, the device does not clear user entries when receiving DHCP Release packets from MAC address authentication users.

Format

mac-authen offline dhcp-release

undo mac-authen offline dhcp-release

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MAC address authentication users who send DHCP Release packets go offline, the corresponding user entries on the device cannot be deleted immediately. This occupies device resources and possibly prevents other users from

going online. You can run this command to enable the device to clear the user entries in real time when MAC address authentication users go offline.

Precautions

MAC address authentication users who go online through VLANIF interfaces do not support this function.

If the device functions as a DHCP relay agent, configure the DHCP snooping function on the device; otherwise, this command does not take effect.

Example

In the MAC access profile **m1**, enable the device to clear user entries when receiving DHCP Release packets from MAC address authentication users.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] mac-authen offline dhcp-release
```

13.5.179 mac-authen permit mac-address

Function

The **mac-authen permit mac-address** command specifies the MAC address range allowed for MAC address authentication.

The **undo mac-authen permit mac-address** command deletes the MAC address range allowed for MAC address authentication.

By default, no MAC address range is specified for MAC address authentication.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

undo mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address for MAC address authentication.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the MAC address mask.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.

Parameter	Description	Value
mask *mask-length*	Specifies the MAC address mask length.	The value is an integer that ranges from 1 to 48.

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a new MAC address entry is generated on the device after MAC address authentication is enabled on a VLANIF interface, MAC address authentication will be performed for the corresponding user. To actually control the users who can be authenticated using MAC addresses on the VLANIF interface, use this command to specify a MAC address range for MAC address authentication.

Precautions

Only MAC address authentication users who go online through VLANIF interfaces support this function.

A maximum of eight MAC address ranges are allowed for MAC address authentication on a VLANIF interface.

Example

In the MAC access profile **m1**, set the MAC address to 00e0-fc01-0101 and the MAC address mask length to 24 for MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] mac-authen permit mac-address 00e0-fc01-0101 mask 24
```

13.5.180 mac-authen quiet-times

Function

The **mac-authen quiet-times** command configures the maximum number of authentication failures within 60 seconds before a MAC address authentication user enters the quiet state.

The **undo mac-authen quiet-times** command restores the maximum number of authentication failures to the default value.

By default, the maximum number of authentication failures is 10.

Format

mac-authen quiet-times *fail-times*

undo mac-authen quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a MAC address authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The quiet function for MAC address authentication is enabled on a device by default. When the maximum number of authentication failures exceeds 10 within 60 seconds, the device quiets a MAC address authentication user and does not process authentication requests from the user, reducing impact on the system caused by attackers.

Precautions

After the maximum number of authentication failures is set to a value larger than the configured value, the user in quiet state can initiate reauthentication only after the quiet period expires. If the user enters an incorrect user name or password again, the user authentication fails. The device does not quiet the user but allows the user to initiate reauthentication immediately.

The quiet function for MAC address authentication users takes effect only after the pre-connection function is disabled using the **undo authentication pre-authen-access enable** command and the device is disabled from assigning network access rights to users in each phase before authentication succeeds using the **undo authentication event action authorize** command.

Example

Set the maximum number of authentication failures within 60 seconds to 4.


```
<HUAWEI> system-view
[HUAWEI] mac-authen quiet-times 4
```

13.5.181 mac-authen reauthenticate mac-address

Function

The **mac-authen reauthenticate mac-address** command enables re-authentication for an online MAC address authentication user with a specified MAC address.

By default, re-authentication for an online MAC address authentication user with a specified MAC address is disabled.

Format

mac-authen reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies all valid unicast MAC addresses.	The value is in H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **mac-authen reauthenticate**.

The **mac-authen reauthenticate mac-address** and **mac-authen reauthenticate** commands re-authenticate online MAC address authentication users and their difference is as follows:

- The **mac-authen reauthenticate mac-address** command configures the device to immediately re-authenticate a user with a specified MAC address for once.
- The **mac-authen reauthenticate** command configures the device to re-authenticate all online MAC address authentication users at intervals.
- The **mac-authen reauthenticate mac-address** command does not support re-authentication for MAC address authentication users in pre-connection state.

Example

Enable re-authentication for an online MAC address authentication user with the MAC address 00e0-fc02-0003.

```
<HUAWEI> system-view
[HUAWEI] mac-authen reauthenticate mac-address 00e0-fc12-3456
```

13.5.182 mac-authen reauthenticate

Function

The **mac-authen reauthenticate** command enables re-authentication for online MAC address authentication users.

The **undo mac-authen reauthenticate** command restores the default configuration.

By default, re-authentication for online MAC address authentication users is disabled.

Format

mac-authen reauthenticate

undo mac-authen reauthenticate

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the administrator modifies the authentication parameters of an online user on the authentication server, the user must be re-authenticated to ensure user validity.

After the user goes online, the device saves authentication parameters of the user. After re-authentication is configured for online MAC address authentication users, the device automatically sends the user authentication parameters in the MAC access profile to the authentication server at an interval (specified using the **mac-authen timer reauthenticate-period** command) for re-authentication. If the user authentication information on the authentication server remains unchanged, the users are kept online. If the information has been changed, the users are disconnected and need to be re-authenticated based on the changed authentication parameters.

Precautions

After periodic re-authentication is configured for online MAC address authentication users, a large number of MAC address authentication logs are generated.

This function takes effect only for users who go online after this function is successfully configured.

MAC address authentication users who go online through a VLANIF interface do not support re-authentication.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Example

In the MAC access profile **mac_access_profile**, configure re-authentication for online MAC address authentication users.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] mac-authen reauthenticate
```

13.5.183 mac-authen reauthenticate dhcp-renew

Function

The **mac-authen reauthenticate dhcp-renew** command enables the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

The **undo mac-authen reauthenticate dhcp-renew** command restores the default setting.

By default, the device does not re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

Format

mac-authen reauthenticate dhcp-renew

undo mac-authen reauthenticate dhcp-renew

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After users go online, the administrator may modify the users' authentication parameters or network access rights on the authentication server. To ensure user validity or update the users' network access rights in real time, you can run this command to enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

Precautions

MAC address authentication users who go online through a VLANIF interface do not support re-authentication.

This function applies only to Layer 2 BNG scenarios.

Example

In the MAC access profile **m1**, enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] mac-authen reauthenticate dhcp-renew
```

13.5.184 mac-authen timer quiet-period

Function

The **mac-authen timer quiet-period** command configures the quiet period for MAC address authentication users who fail to be authenticated.

The **undo mac-authen timer quiet-period** command restores the default quiet period.

By default, the quiet period is 60 seconds for MAC address authentication users who fail to be authenticated.

Format

mac-authen timer quiet-period *quiet-period-value*

undo mac-authen timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-value	Sets the quiet period for MAC address authentication users who fail to be authenticated.	The value is an integer that ranges from 0 to 3600, in seconds. **NOTE** If the value of *quiet-period-value* is 0, the quiet function is disabled for MAC address authentication users.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a MAC address authentication user fails to be authenticated consecutively within a short period, the system is affected and a large number of duplicated authentication failure logs are generated.

After the quiet function is enabled, if the number of times that a MAC address authentication user fails to be authenticated within 60s exceeds the upper limit (configured using the **mac-authen quiet-times** command), the device discards the user's MAC address authentication request packets for a period to avoid frequent authentication failures.

NOTE

The quiet function for MAC address authentication users takes effect only after the pre-connection function is disabled using the **undo authentication pre-authen-access enable** command and the device is disabled from assigning network access rights to users in each phase before authentication succeeds using the **undo authentication event action authorize** command.

Example

Set the quiet period to 100 seconds for MAC address authentication users who fail to be authenticated.

```
<HUAWEI> system-view
[HUAWEI] mac-authen timer quiet-period 100
```


13.5.185 mac-authen timer reauthenticate-period

Function

The **mac-authen timer reauthenticate-period** command configures the re-authentication interval for online MAC address authentication users.

The **undo mac-authen timer reauthenticate-period** command restores the default setting.

By default, the re-authentication period is 1800 seconds for online MAC address authentication users.

Format

mac-authen timer reauthenticate-period *reauthenticate-period-value*

undo mac-authen timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the interval for re-authenticating online MAC address authentication users.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring the re-authentication function for online MAC address authentication users using the **mac-authen reauthenticate** command, run the **mac-authen timer reauthenticate-period** command to configure the re-authentication interval. The device then re-authenticates online users at the specified interval, ensuring that only authorized users can keep online.

Precautions

Generally, the default re-authentication interval is recommended. If many ACL rules need to be delivered during user authorization, to improve the device processing performance, you are advised to disable re-authentication or increase the re-authentication internal. When remote authentication and authorization are

used and a short re-authentication interval is used, the CPU usage may become high.

MAC address authentication users who go online through a VLANIF interface do not support re-authentication.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

In the MAC access profile **mac_access_profile**, configure the re-authentication interval for online MAC address authentication users to 2000 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] mac-authen timer reauthenticate-period 2000
```

13.5.186 mac-authen trigger dhcp-binding

Function

The **mac-authen trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-connection phase.

The **undo mac-authen trigger dhcp-binding** command restores the default configuration.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-authentication phase.

Format

mac-authen trigger dhcp-binding

undo mac-authen trigger dhcp-binding

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through MAC address authentication, the unauthorized users can obtain the same identities as the authorized users. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting normal communication between authorized users. To prevent the previous attacks, configure IPSG. This function is implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After this function is enabled, the device automatically generates the DHCP snooping binding table based on the MAC address, IP address, and interface information of static IP users who pass MAC address authentication or are at the pre-authentication phase.

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass MAC address authentication or are at the pre-authentication phase. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.

Precautions

- To make this function take effect, you must run the **dhcp snooping enable** command on the interface to which the mac access profile is bound to enable the DHCP snooping function on the interface and globally.
- The authentication profile bound to the MAC access profile in which the command is configured must be applied to a Layer 2 interface. If the authentication profile is applied to a Layer 3 interface, the command does not take effect.
- For users who are assigned IP addresses using DHCP, you do not need to run the **mac-authen trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function. For static IP users (for example, users who trigger authentication by sending ARP packets carrying IP addresses), run the **mac-authen trigger dhcp-binding** command and configure DHCP snooping on the device to generate DHCP snooping binding entries.
- The IP address in the DHCP snooping binding table is extracted from the ARP request packet (the first ARP request packet sent by the user after the user is authenticated or in the pre-connection state that has the same MAC address in the user information table).
- This function trusts only the first ARP packet in the authentication process. If a client sends an ARP packet with a non-static IP address during authentication and then sends an ARP packet with the real IP address, the

DHCP snooping binding table is not updated. After this function is enabled, online users cannot change their static IP addresses. If the static IP address of a user is changed, the user needs to be authenticated again.

Example

In the MAC access profile **m1**, enable the device to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-authentication phase.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] mac-authen trigger dhcp-binding
```

13.5.187 mac-authen username

Function

The **mac-authen username** command configures the user name for MAC address authentication.

The **undo mac-authen username** command restores the default setting.

By default, the MAC address without hyphens (-) or colons (:) is used as the user name and password for MAC address authentication.

Format

mac-authen username { **fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]] | **dhcp-option** *option-code* { **circuit-id** | **remote-id** } * [**separate** *separate*] [**format-hex**] **password cipher** *password* }

undo mac-authen username [**fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]] | **dhcp-option** *option-code* [**circuit-id** | **remote-id**] * [**password cipher** *password*]]

Parameters

Parameter	Description	Value
fixed *username*	Specifies a fixed user name for MAC address authentication.	The value is a string of 1 to 64 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
password cipher *password*	Specifies the password in cipher text for MAC address authentication. • You do not need to set a password for a fixed user name if the authentication mode is none. In this case, the user can log in without a password. However, this poses security risks and is not recommended. • If no password is set when the MAC address is used as the user name, the user can log in using the MAC address as the password. A password must be configured when local authentication is used in the AAA scheme. • The password must be configured when the user name for MAC address authentication is in the DHCP option format.	The value is a string of case-sensitive characters without spaces. The password is either a plain-text string of 1 to 128 characters or a cipher-text string of 48 to 188 characters. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** For security purposes, change the default password in real time. The new password must be a combination of at least two of the following: digits, lowercase letters, uppercase letters, and special characters. In addition, the password must consist of six or more than eight characters.

Parameter	Description	Value
macaddress	Specifies the MAC address as the user name for MAC address authentication.	-
format { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** }	Specifies the MAC address format. • **with-hyphen**: indicates that the MAC address contains hyphens (-), the format is xxxx-xxxx-xxxx. • **with-hyphen normal**: indicates that the MAC address contains hyphens (-), the format is xx-xx-xx-xx-xx-xx. • **with-hyphen colon**: indicates that the MAC address contains colons (:), the format is xxxx:xxxx:xxxx. • **with-hyphen normal colon**: indicates that the MAC address contains colons (:), the format is xx:xx:xx:xx:xx:xx. • **without-hyphen**: indicates that the MAC address does not contain hyphens (-) or colons (:), the format is xxxxxxxxxxxx.	-
uppercase	Indicates that the name of a MAC address authentication user is in uppercase.	-
dhcp-option *option-code*	Specifies the name of the MAC address authentication user to a specified DHCP option. • **circuit-id**: Specifies the circuit ID in the DHCP Option82 field as the user name in MAC address authentication. • **remote-id**: Specifies the remote ID in the DHCP Option82 field as the user name in MAC address authentication. If both **circuit-id** and **remote-id** are configured, the user name for MAC address authentication can be set to a character string that is a combination of the **circuit-id** and **remote-id** in the DHCP Option82 field.	The value is an integer. In the current version, the value is fixed as 82.

Parameter	Description	Value
separate *separate*	Specifies the delimiter in the user name for MAC address authentication. This parameter is configured when the user name for MAC address authentication is set to a character string that is a combination of the **circuit-id** and **remote-id** in the DHCP Option82 field.	The value is a character and can be set to a letter, digit, or another valid character.
format-hex	Indicates that the user name for MAC address authentication is in hexadecimal format.	-

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following user name formats are available for MAC address authentication:

- Fixed user name: A user uses the fixed user name and password configured by the administrator for authentication.
- MAC address: A user uses the MAC address as the user name for authentication. In addition, the MAC address or user-defined character string can be used as the password.
- When the DHCP option format is used for MAC address authentication, the device uses the DHCP option it obtains and password set by the administrator for authentication. In this mode, ensure that the device supports MAC address authentication triggered through DHCP packets.

By default, the device sends the user MAC address as the user name and password to the authentication server for authentication. However, the users cannot be easily identified and managed in this case. To flexibly identify and manage users, run the **mac-authen username** command to configure fixed user names and passwords for MAC address authentication users.

Precautions

- When configuring the user name format for MAC address authentication, ensure that the authentication server supports the user name format.
- If MAC address authentication is enabled on a VLANIF interface, on an Eth-Trunk, in a port group, or in a VAP profile, and MAC address authentication users use fixed user names, passwords must be configured. If MAC address

authentication is enabled in a port group and MAC addresses are used as user names, passwords cannot be configured. If MAC address authentication is enabled on a VLANIF interface or in a VAP profile, user names for MAC address authentication cannot be set to specified DHCP option information.

Example

In the MAC access profile **mac_access_profile**, configure the device to use the MAC address containing hyphens (-) as the user name.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] mac-authen username macaddress format with-hyphen
```

13.5.188 match access-context-profile action

Function

The **match access-context-profile action** command configures the network access rights for specified users in each phase before authentication success based on user context profiles.

The **undo match access-context-profile action** command deletes the configured network access rights.

By default, no network access right is configured for specified users in each phase before authentication success.

Format

match access-context-profile *profile-name* **action** { **authen-fail service-scheme** *service-scheme-name* | **authen-server-down service-scheme** *service-scheme-name* | **authen-server-up re-authen** | **client-no-response service-scheme** *service-scheme-name* | **portal-server-down service-scheme** *service-scheme-name* | **portal-server-up re-authen** | **pre-authen service-scheme** *service-scheme-name* } *

undo match access-context-profile *profile-name* **action** { **authen-fail** | **authen-server-down** | **authen-server-up** | **client-no-response** | **portal-server-down** | **portal-server-up** | **pre-authen** } *

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a user context profile.	The value must be the name of an existing user context profile.

Parameter	Description	Value
authen-fail	Configures the device to assign network access rights to users when the authentication server sends authentication failure packets to the device.	-
authen-server-down	Configures the device to assign network access rights to users when the authentication server is unreachable and thereby the users fail to be authenticated.	-
authen-server-up	Re-authenticates users when the authentication server can be reachable again.	-
client-no-response	Configures the device to assign network access rights to users when clients do not respond and thereby the users fail to be authenticated.	-
portal-server-down	Configures the device to assign network access rights to users when the Portal server is unreachable and thereby the users fail to be authenticated.	-
portal-server-up	Re-authenticates users when the Portal server can be reachable again.	-
pre-authen	Configures the device to assign network access rights to users when the users establish pre-connections with the device.	-
re-authen	Re-initializes user rights.	-
service-scheme *service-scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to users.	The value must be the name of an existing service scheme name on the device.

Views

User authentication event authorization policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users need basic network access rights before they are authenticated. For example, the users need to download 802.1X clients and update the antivirus database. A user authentication event authorization policy can be used to bind the network access rights of users in each phase before authentication success to a user context profile. When a user goes online after a user authentication event authorization policy is applied to the device, the device adds the user to the context profile based on the user context identification result, and assigns the network access rights to the user based on the user authentication result. The **match access-context-profile action** command can be used to configure the network access rights for users in each phase (including an authentication failure, an authentication server fault, and no response from the users) before authentication success.

Prerequisites

- A service scheme has been created using the **service-scheme** command in the AAA view.
- A user context profile has been created using the **access-context profile name** *profile-name* command in the system view.

Follow-up Procedure

In the global view, run the **access-author policy global** command to apply the user authentication event authorization policy.

Precautions

The priority of user authorization based on a user context profile is higher than that of user authorization in an authentication profile.

This function takes effect only for users who go online after this function is successfully configured.

Example

Match the user authentication event authorization policy **a1** with the identification result of the user context profile **p1**, and use the service scheme **s1** to authorize the users who fail to be authenticated.

```
<HUAWEI> system-view
[HUAWEI] access-context profile name p1
[HUAWEI-access-context-p1] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] quit
[HUAWEI-aaa] quit
[HUAWEI] access-author policy name a1
[HUAWEI-access-author-a1] match access-context-profile p1 action authen-fail service-scheme s1
```


13.5.189 match access-context-profile action access-domain

Function

The **match access-context-profile action access-domain** command configures the access user's authentication domain based on the user context profile.

The **undo match access-context-profile action access-domain** command deletes the access user's authentication domain based on the user context profile.

By default, no access user's authentication domain is configured based on the user context profile.

Format

match access-context-profile *profile-name* **action access-domain** *domain-name* [**dot1x** | **mac-authen** | **portal**] * [**force**]

undo match access-context-profile *profile-name* **action access-domain** [**dot1x** | **mac-authen** | **portal**] * [**force**]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the matching user context profile.	The value must be the name of an existing user context profile.
domain-name	Specifies the domain name.	The value must be the name of an existing domain on the device.
dot1x	Specifies a default or forcible domain for 802.1X authentication users.	-
mac-authen	Specifies a default or forcible domain for MAC address authentication users.	-
portal	Specifies a default or forcible domain for Portal authentication users.	-
force	Specifies the configured domain as a forcible domain. If this parameter is not specified, the configured domain is a default domain.	-

Views

User authentication event authorization policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some enterprise networks, VLAN is divided into multiple areas with different security levels. The administrator assigns different network access rights to access users in different areas. The device uses the domain to manage users, so the access user's authentication domain can be configured based on the user context profile. Based on different context profiles matching with access VLANs, users in different areas have different authentication domains and are assigned different network access rights.

Prerequisites

- A domain has been configured using the **domain** command in the AAA view.
- A user context profile has been configured using the **access-context profile name** *profile-name* command in the system view.

Precautions

The priorities of the forcible domain, domain carried in the user name, and default domain in different views are as follows in descending order: forcible domain with a specified authentication mode in an authentication profile > forcible domain in an authentication profile > forcible domain with a specified authentication mode based on a user context profile > forcible domain based on a user context profile > domain carried in the user name > default domain with a specified authentication mode in an authentication profile > default domain in an authentication profile > default domain with a specified authentication mode based on a user context profile > default domain based on a user context profile > global default domain.

Example

In the user authentication event authorization policy view, configure the user's forcible domain **test** based on the user context profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] quit
[HUAWEI-aaa] quit
[HUAWEI] access-context profile name p1
[HUAWEI-access-context-p1] quit
[HUAWEI] access-author policy name a1
[HUAWEI-access-author-a1] match access-context-profile p1 action access-domain test force
```


13.5.190 mdns snooping enable

Function

The **mdns snooping enable** command enables the mDNS snooping function.

The **undo mdns snooping enable** command disables the mDNS snooping function.

By default, mDNS snooping is disabled.

Format

mdns snooping enable

undo mdns snooping enable

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, VLAN view, Eth-Trunk interface view, port group view.

Default Level

2: Configuration level

Usage Guidelines

In terminal type identification scenarios, if the IP address, MAC address, and service name of a terminal need to be identified based on information in the mDNS packets sent by the terminal, run the **mdns snooping enable** command to enable mDNS snooping on the device. After mDNS snooping is enabled, the device obtains the preceding information and reports it to the controller.

This command cannot be configured on Layer 3 interfaces.

Example

Enable mDNS snooping.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mdns snooping enable
```

13.5.191 parameter

Function

The **parameter** command configures the characters used in URL.

The **undo parameter** command restores the default settings.

By default, the start character of URL parameters is a question mark (?), the assignment character of URL parameters is an equal sign (=), and the delimiter between URL parameters is an ampersand (&).

Format

parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

undo parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

Parameters

Parameter	Description	Value
start-mark *parameter-value*	Specifies the start character for URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
assignment-mark *parameter-value*	Specifies the assignment character for URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
isolate-mark *parameter-value*	Specifies the delimiter between URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

You can run the **parameter** command to modify the characters in URLs.

By default, the start character of URL parameters is a question mark (?), the assignment character of URL parameters is an equal sign (=), and the delimiter between URL parameters is an ampersand (&). However, the **url (URL template view)** command does not support a URL containing a question mark (?). Therefore, you can replace the question mark (?) in a URL with another character in the **url (URL template view)** command configuration, and then run the **parameter start-mark** *parameter-value* command to specify this replacement character as the start character of URL parameters.

In the following example, the replacement character is a number sign (#).

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.11:8080/portal#device-ip=10.1.1.22
[HUAWEI-url-template-test] parameter start-mark #
[HUAWEI-url-template-test] url-parameter user-mac umac user-ipaddress uaddress
```

Processing on the device is as follows:

1. The device automatically replaces the first number sign (#) in the URL with the start character of URL parameters — a question mark (?), and adds a parameter separator "&" at the end of the URL. If the URL does not contain a number sign (#), a question mark (?), instead of an ampersand (&), is added to the end of the URL.
2. The device adds parameters configured by the **url-parameter** command to the end of the URL. The resulting redirect URL is http://10.1.1.11:8080/portal?device-ip=10.1.1.22&umac=00e0-fc02-0002&uaddress=192.168.1.16.

Example

Set the start character for URL parameters to a number sign (#).

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] parameter start-mark #
```

13.5.192 pki key-pair-with-cert

Function

The **pki key-pair-with-cert** command configures the certificate file to be loaded on an AP when the AP is authenticated as an 802.1X client.

The **undo pki key-pair-with-cert** command deletes the certificate file to be loaded on an AP when the AP is authenticated as an 802.1X client.

By default, the certificate file to be loaded on an AP when the AP is authenticated as an 802.1X client is not configured.

Format

pki key-pair-with-cert file-format { **pkcs12** | **pem** } **filename** *filename* **password** *password*

undo pki key-pair-with-cert

NOTE

This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Parameters

Parameter	Description	Value
file-format pkcs12	Indicates that the format of a certificate file is PKCS12.	-
file-format pem	Indicates that the format of a certificate file is PEM.	-
filename *filename*	Specifies the name of a certificate file.	The value is a string of 1 to 63 characters.
password *password*	Specifies the password of a certificate file.	The password can be in plain text or cipher text. ● A plain text password is a string of 6 to 32 characters. ● A cipher text password is a string of 48 or 68 characters that must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an AP is authenticated as an 802.1X client using TLS, you need to load a certificate file on the AP. You can run this command to configure a certificate file. After the AP goes online, the AC automatically delivers the certificate file to the AP.

Precautions

If the certificate file is modified or deleted, or a certificate file is added after the AP goes online, the AC cannot automatically deliver the certificate file again. In this case, you can run the **load-file (WLAN view)** command to manually deliver the certificate file to the AP.

Example

Configure the certificate file to be loaded on an AP when the AP is authenticated as an 802.1X client. Set the format, name, and password of the certificate file to **PEM**, **serverlocal.pem**, and YsHsjx_202206, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap_system1
[HUAWEI-wlan-ap-system-prof-ap_system1] pki key-pair-with-cert file-format pem filename
serverlocal.pem password YsHsjx_202206
```

13.5.193 pki-realm

Function

The **pki-realm** command configures the PKI realm used for TLS authentication.

The **undo pki-realm** command deletes the PKI realm used for TLS authentication.

By default, no PKI realm is configured for TLS authentication.

NOTE

Only the following models support this command:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

pki-realm *pki-realm*

undo pki-realm

Parameters

Parameter	Description	Value
pki-realm *pki-realm*	Specifies the PKI realm used for TLS authentication. The name of the PKI realm must be **user-define** or **default**.	The value is a string of 1 to 64 characters. **NOTE** If the specified PKI domain is the default domain, there may be security risks.

Views

802.1X client profile view

Default Level

2: Configuration level

Usage Guidelines

When the device functions as an 802.1X client and uses TLS authentication, you can run this command to configure a PKI realm for loading the digital certificate on the 802.1X client.

This configuration will not be delivered to APs.

Example

Configure a PKI realm used for TLS authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name d1
[HUAWEI-dot1x-client-profile-d1] pki-realm user-define
```

13.5.194 port (Portal server template view)

Function

The **port** command sets the port number that a Portal server uses to receive notification packets from the device.

The **undo port** command restores the default port number.

By default, a Portal server uses port number 50100 to receive packets from the device.

Format

port *port-number* [**all**]

undo port [**all**]

Parameters

Parameter	Description	Value
port-number	Specifies the port number that the Portal server uses to receive and encapsulate UDP packets from the device.	The value is an integer that ranges from 1 to 65535. By default, the value is 50100.

Parameter	Description	Value
all	Indicates that the device always uses the destination port number specified by *port-number* to encapsulate UDP packets. **NOTE** After this keyword is specified, when receiving UDP packets from a Portal server, the device does not obtain the source port number in the UDP packets as the destination port number of UDP packets to be sent to the Portal server. If the value of *port-number* is different from the source port number of the Portal server, the Portal server cannot receive the UDP packets sent by the device. Therefore, this keyword is not recommended.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server template on the device using the **web-auth-server** command, configure parameters for the template.

Run the **port** command to set the port number that a Portal server uses to receive notification packets from the device. After receiving a Portal authentication request packet from a user, the device sends the packet to the Portal server using the specified destination port number.

Precautions

Ensure that the port number configured on the device is the same as that used by the Portal server.

Example

Set the port number that a Portal server uses to receive packets from the device to 10000 in the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] port 10000
```

13.5.195 portal auth-network

Function

The **portal auth-network** command configures the source subnet for Portal authentication.

The **undo portal auth-network** command restores the default setting.

By default, the source subnet for Portal authentication is 0.0.0.0/0, indicating that users in all subnets must pass Portal authentication.

Format

portal auth-network *network-address* { *mask-length* | *mask-address* }

undo portal auth-network { *network-address* { *mask-length* | *mask-address* } | **all** }

Parameters

Parameter	Description	Value
network-address	Specifies a Portal authentication subnet.	The value is in dotted decimal notation.
mask-length | *mask-address*	Specifies the mask length or mask of the Portal authentication subnet. • *mask-length*: specifies the mask length. • *mask-address*: specifies the mask.	• The value of *mask-length* is an integer that ranges from 1 to 32. • The value of *mask-address* is in dotted decimal notation.
all	Deletes all Portal authentication subnets.	-

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source subnet for Portal authentication is configured, only user packets from the subnet can trigger Portal authentication. If an unauthenticated user is not on a Portal authentication subnet and packets from the user do not match any Portal authentication-free rule, the device discards the user's packets.

Precautions

The command takes effect only for Layer 3 Portal authentication. In Layer 2 Portal authentication, users on all subnets must be authenticated.

Example

In the Portal access profile **p1**, set the source authentication subnet to 10.1.1.0/24.

```
<HUAWEI> system-view
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] portal auth-network 10.1.1.0 24
```

13.5.196 portal captive-adaptive enable

Function

The **portal captive-adaptive enable** command enables the Captive Network Assistant (CNA) adaptive function for iOS terminals.

The **undo portal captive-adaptive enable** command disables the CNA adaptive function for iOS terminals.

By default, the CNA adaptive function is disabled for iOS terminals.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

portal captive-adaptive enable

undo portal captive-adaptive enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

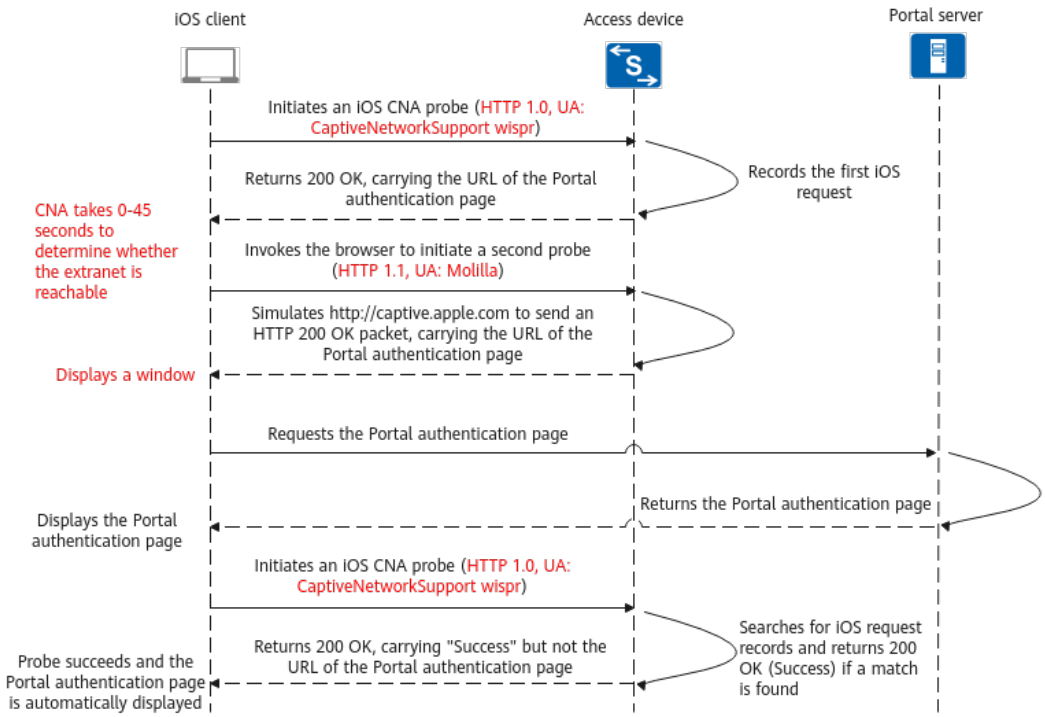
When a user uses an iOS terminal (iPhone, iPad, or iMac) to connect to a WLAN, the CNA of the iOS terminal detects connectivity to http://captive.apple.com. If the network connectivity is normal, the iOS terminal will receive a response indicating success. Otherwise, the iOS terminal invokes the browser to perform a probe again and automatically displays the authentication page. The specific process is as follows:

1. After the terminal associates with an SSID, it sends an HTTP 1.0 request to http://captive.apple.com. The **User-Agent** field in the packet is **CaptiveNetworkSupport wispr**.

2. If the pushed page is not the expected http://www.apple.com/library/test/success.html, the terminal considers a network connection failure and invokes the browser to send an HTTP 1.1 request packet to http://captive.apple.com. The **User-Agent** field in the packet is as follows: **Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_3 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Mobile/13G34**. The field value may slightly vary according to iOS terminals and versions.
3. The Portal authentication page is automatically displayed on the terminal. After the user enters the user name and password, the terminal connects to the WLAN.

The preceding describes the implementation of the CNA mechanism on iOS terminals. Whether the browser can re-send an HTTP request (in step 2) is the key to automatically pushing the Portal authentication page. If the browser is not invoked or is invoked after a long delay, the Portal authentication page will fail to be pushed or will be pushed after a long time. **Figure 13-1** shows the CNA process.

Figure 13-1 CNA process of an iOS terminal



If the CNA probe of an iOS terminal fails, there will be no Wi-Fi symbol on the iOS terminal. You can use either of the following methods to resolve this problem:

- Method 1: Run the **portal captive-bypass enable** command in the system view to enable the device to construct a response carrying **Success** for all requests with the **User-Agent** field being **CaptiveNetworkSupport wispr**. In this way, iOS terminals consider that the network is connected and display the Wi-Fi symbol. The disadvantage of this configuration is that the authentication page cannot be automatically displayed on iOS terminals. Users need to manually open the browser to access a website so that the authentication page can be displayed through redirection.

- Method 2: Run the **portal captive-adaptive enable** command in the system view to enable the device to perform a probe and redirection for the first request with the **User-Agent** field being **CaptiveNetworkSupport wispr** and return a Success (200 OK) message for subsequent requests with the **User-Agent** field being **CaptiveNetworkSupport wispr**. In this way, iOS terminals can automatically display the authentication page and show the Wi-Fi symbol.

Precautions

When applications on iOS mobile terminals are used to perform Portal authentication, you can run only the **portal captive-bypass enable** command to enable the CNA bypass function. After this function is enabled, users who have logged in to the applications can be automatically authenticated and connect to networks, without entering their user names and passwords.

If you run both the **portal captive-adaptive enable** and **portal captive-bypass enable** commands, the command executed later takes effect.

Due to restrictions of iOS 9.3.1, mobile terminals using iOS 9.3.1 cannot connect to WLANs after the CNA adaptive function is enabled. To solve this problem, run the **portal captive-bypass enable** command to enable the CNA bypass function. Terminal users then can be redirected to the application-based Portal authentication page after they open the browser and access a web page.

Authentication-free resources accessed by users cannot contain the URL captive.apple.com; otherwise, terminals cannot automatically display the Portal authentication page.

If the Portal authentication page is of the HTTPS type, terminals can automatically display the Portal authentication page only when an HTTPS URL is used and the domain name certificate is valid.

Example

Enable the CNA adaptive function for iOS terminals.

```
<HUAWEI> system-view
[HUAWEI] portal captive-adaptive enable
```

13.5.197 portal captive-bypass enable

Function

The **portal captive-bypass enable** command enables the CNA bypass function for iOS terminals.

The **undo portal captive-bypass enable** command disables the CNA bypass function.

By default, the CNA bypass function is disabled for iOS terminals.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

portal captive-bypass enable

undo portal captive-bypass enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The iOS operating system provides the Captive Network Assistant (CNA) function. With the CNA function, the iOS terminals (including iPhone, iPad, and iMAC) automatically detects wireless network connectivity after associating with a wireless network. If the network connection cannot be set up, the iOS terminals ask users to enter user names and passwords. If users do not enter the user names and passwords, the iOS terminals automatically disconnect from the wireless network.

However, Portal authentication allows users to access certain resources before authentication is successful. If the iOS terminals are disconnected, users cannot access the specified resources. The CNA bypass function addresses this problem. If the users do not enter user names and passwords immediately, the CNA bypass function keeps the iOS terminals online before the Portal authentication is successful. Therefore, the iOS users are allowed to access authentication-free resources.

Precautions

After the CNA bypass function is enabled for iOS terminals, the Portal authentication page will not be automatically displayed for iOS terminals.

Example

Enable the CNA bypass function for iOS terminals.

```
<HUAWEI> system-view
[HUAWEI] portal captive-bypass enable
```

13.5.198 portal https-redirect blacklist

Function

The **portal https-redirect blacklist** command adds an address to the HTTPS redirection blacklist. After an address is added to the HTTPS redirection blacklist,

HTTPS redirection is not performed for HTTPS access to this address of Portal users.

The **undo portal https-redirect blacklist** command removes an address from the HTTPS redirection blacklist.

By default, no address is added to the HTTPS redirection blacklist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist ip *start-ip-address* [*end-ip-address*]

portal https-redirect blacklist ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]

undo portal https-redirect blacklist ip { *start-ip-address* [*end-ip-address*] | **all** }

undo portal https-redirect blacklist ipv6 { *start-ipv6-address* [**to** *end-ipv6-address*] | **all** }

Parameters

Parameter	Description	Value
ip *start-ip-address* [*end-ip-address*]	Specifies an IPv4 address or an IPv4 address range: • *start-ip-address* specifies the start IPv4 address. • *end-ip-address* specifies the end IPv4 address.	-
ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]	Specifies an IPv6 address or an IPv6 address range: • *start-ipv6-address* specifies the start IPv6 address. • *end-ipv6-address* specifies the end IPv6 address.	-
all	Removes all IPv4 addresses or IPv6 addresses from the HTTPS redirection blacklist.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before users pass Portal authentication, HTTPS access to a website other than the Portal server triggers HTTPS redirection by default. To disable HTTPS redirection for HTTPS access to a specified address, run the **portal https-redirect blacklist** command to add this address to the HTTPS redirection blacklist.

Precautions

If an address has been added to the HTTPS redirection whitelist using the **portal https-redirect whitelist** command, this address cannot be added to the HTTPS redirection blacklist.

If an address (except the address of the Portal server) is not in the HTTPS redirection blacklist, HTTPS access to this address will always trigger HTTPS redirection before users pass Portal authentication.

Example

Add 10.1.1.1 to the HTTPS redirection blacklist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist ip 10.1.1.1
```

Add FC00::1 to the HTTPS redirection blacklist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist ipv6 FC00::1
```

13.5.199 portal https-redirect blacklist aging-time

Function

The **portal https-redirect blacklist aging-time** command configures the aging time of addresses in the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist aging-time** command restores the default aging time of addresses in the HTTPS redirection blacklist.

By default, the aging time of addresses in the HTTPS redirection blacklist is 259200 seconds, that is, 72 hours.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist aging-time *aging-time*

undo portal https-redirect blacklist aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of addresses in the HTTPS redirection blacklist.	The value is an integer in the range from 30 to 4294967295, in seconds. The default value is 259200 seconds, that is, 72 hours.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After an address (except the address of the Portal server) is added to the HTTPS redirection blacklist, HTTPS access from Portal users to this address does not trigger HTTPS redirection. By default, the aging time of addresses in the HTTPS redirection blacklist is 259200 seconds. When the aging time expires, this address will be removed from the blacklist. You can use the **portal https-redirect blacklist aging-time** command to adjust the aging time of addresses in the HTTPS redirection blacklist.

Example

Configure the aging time of addresses in the HTTPS redirection blacklist to 86400 seconds, that is, 24 hours.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist aging-time 86400
```

13.5.200 portal https-redirect blacklist packet-rate

Function

The **portal https-redirect blacklist packet-rate** command configures the maximum rate at which a Portal user accesses an address through HTTPS. If the user access rate reaches the maximum, the switch adds the destination address to the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist packet-rate** command restores the default maximum rate at which a Portal user accesses an address through HTTPS.

By default, the maximum rate at which a Portal user accesses an address through HTTPS is 40 times per minute.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist packet-rate *packet-rate*

undo portal https-redirect blacklist packet-rate

Parameters

Parameter	Description	Value
packet-rate	Specifies the maximum rate at which a Portal user accesses an address through HTTPS.	The value is an integer in the range from 5 to 600, in times per minutes. The default value is 40.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the switch redirects the HTTP or HTTPS requests sent from clients to the Portal login page. When the rate of packets sent from a Portal user for accessing an address through HTTPS reaches the maximum rate specified by the **portal https-redirect blacklist packet-rate** command, the switch adds the destination address to the HTTPS redirection blacklist. This prevents repeated HTTPS redirection caused by frequent access from malicious users to an address, and therefore saves resources of the switch.

Prerequisites

The function of inserting a JavaScript file during Portal redirection has been enabled using the **portal redirect js enable** command.

Precautions

This command takes effect only for the HTTPS protocol.

This command takes effect for both IPv4 and IPv6 addresses.

Example

Set the maximum rate at which a Portal user accesses an address through HTTPS to 30 times per minute.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist packet-rate 30
```

13.5.201 portal https-redirect blacklist retry-times interval

Function

The **portal https-redirect blacklist retry-times interval** command configures the maximum number of times and the detection period. Within the detection period, if the number of times an address is added to the provisional HTTPS redirection blacklist reaches the maximum, the address is added to the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist retry-times interval** command restores the default maximum number of times and the default detection period.

By default, the maximum number of times is 10 and the detection period is 3 minutes.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist retry-times *retry-times* **interval** *interval*

undo portal https-redirect blacklist retry-times interval

Parameters

Parameter	Description	Value
retry-times	Specifies the maximum number of times.	The value is an integer in the range from 1 to 600. The default value is 10.
interval	Specifies the detection period.	The value is an integer in the range from 1 to 600, in minutes. The default value is 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the switch redirects the HTTP or HTTPS requests sent from clients to the Portal login page. When the function of inserting a JavaScript file during Portal redirection is enabled on the switch using the **portal redirect js enable** command, the HTTP or HTTPS response packets sent from the switch to clients carry the JavaScript file.

- The clients can be redirected to the Portal login page only after they correctly parse the JavaScript file.
- If a client fails to parse the JavaScript file, the switch adds the destination address to the provisional HTTPS redirection blacklist. HTTP and HTTPS redirection can still be triggered for addresses in the provisional HTTPS redirection blacklist.

The detection period specified in the **portal https-redirect blacklist retry-times interval** command starts from the time when an address is added to the provisional HTTPS redirection blacklist. If the number of times an address is added to the provisional HTTPS redirection blacklist reaches the maximum within the detection period, this address is added to the HTTPS redirection blacklist.

Precautions

This command takes effect only for the HTTPS protocol.

This command takes effect for both IPv4 and IPv6 addresses.

Example

Set the maximum number of times to 15 and the detection period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist retry-times 15 interval 5
```

13.5.202 portal https-redirect tls1.1 enable

Function

The **portal https-redirect tls1.1 enable** command configures TLS 1.1 for HTTPS redirection in Portal authentication.

The **undo portal https-redirect tls1.1 enable** command cancels the configuration.

By default, TLS 1.2 is used for HTTPS redirection in Portal authentication.

NOTE

Only the following switch models support this command:

S200, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect tls1.1 enable

undo portal https-redirect tls1.1 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used to configure whether the TLS 1.1 protocol is used for HTTPS redirection in Portal authentication.

Precautions

In versions earlier than V200R021C00, the TLS 1.1 protocol is used for HTTPS redirection in Portal authentication by default; however, the TLS 1.2 protocol is used by default in V200R021C00 and later versions. If the device is upgraded from an earlier version to V200R021C00 or later, the **portal https-redirect tls1.1 enable** command is automatically generated in the system configuration file to ensure compatibility.

In V200R021C00, this command takes effect only for wired users. In V200R021C10 and later versions, this command takes effect for both wired and wireless users.

TLS 1.2 is recommended because it is more secure than TLS 1.1.

Example

Configure TLS 1.1 for HTTPS redirection in Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect tls1.1 enable
```


13.5.203 portal https-redirect whitelist

Function

The **portal https-redirect whitelist** command adds an address to the HTTPS redirection whitelist.

The **undo portal https-redirect whitelist** command removes an address from the HTTPS redirection whitelist.

By default, no address is added to the HTTPS redirection whitelist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect whitelist ip *start-ip-address* [*end-ip-address*]

portal https-redirect whitelist ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]

undo portal https-redirect whitelist ip { *start-ip-address* [*end-ip-address*] | **all** }

undo portal https-redirect whitelist ipv6 { *start-ipv6-address* [**to** *end-ipv6-address*] | **all** }

Parameters

Parameter	Description	Value
ip *start-ip-address* [*end-ip-address*]	Specifies an IPv4 address or an IPv4 address range: • *start-ip-address* specifies the start IPv4 address. • *end-ip-address* specifies the end IPv4 address.	-
ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]	Specifies an IPv6 address or an IPv6 address range: • *start-ipv6-address* specifies the start IPv6 address. • *end-ipv6-address* specifies the end IPv6 address.	-

Parameter	Description	Value
all	Removes all IPv4 addresses or IPv6 addresses from the HTTPS redirection whitelist.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before users pass Portal authentication, HTTPS access to a website other than the Portal server triggers HTTPS redirection by default. If an address is added to the HTTPS redirection blacklist by mistake, HTTPS access to this address will not trigger HTTPS redirection. To ensure that HTTPS redirection is performed for HTTPS access to specified addresses, use the **portal https-redirect whitelist** command to add these addresses to the HTTPS redirection whitelist.

Configuration Impact

If an address has been added to the HTTPS redirection whitelist, this address cannot be added to the HTTPS redirection blacklist using the **portal https-redirect blacklist** command.

Precautions

If an address in the HTTPS redirection blacklist is added to the HTTPS redirection whitelist, the switch removes the address from the HTTPS redirection blacklist.

If an address (except the address of the Portal server) is not in the HTTPS redirection blacklist, HTTPS access to this address will always trigger HTTPS redirection before users pass Portal authentication.

Example

Add 10.1.2.1 to the HTTPS redirection whitelist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect whitelist ip 10.1.2.1
```

Add FC00::2 to the HTTPS redirection whitelist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect whitelist ipv6 FC00::2
```


13.5.204 portal https-redirect wired enable

Function

The **portal https-redirect wired enable** command enables HTTPS redirection for wired Portal authentication users.

The **undo portal https-redirect wired enable** command disables HTTPS redirection for wired Portal authentication users.

By default, HTTPS redirection is disabled for wired Portal authentication users.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect wired enable

undo portal https-redirect wired enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After HTTPS redirection is disabled for wired Portal authentication users, Portal authentication cannot be triggered when a wired Portal authentication user uses HTTPS to access a website. As a result, the user cannot go online. To allow Portal authentication be triggered when a wired Portal authentication user uses HTTPS to access a website, run the **portal https-redirect wired enable** command to enable HTTPS redirection for wired Portal authentication users.

Prerequisites

HTTPS redirection of Portal authentication has been enabled using the **authentication https-redirect enable** command.

Configuration Impact

If a non-Huawei AC and non-Huawei APs are connected to the switch, APs and users are associated with the AC, and the switch performs Portal authentication for access users, users will go online at a slow rate after HTTPS redirection is enabled for wired Portal authentication users. Therefore, it is recommended that you disable HTTPS redirection for wired Portal authentication users in this scenario.

Precautions

After HTTPS redirection is disabled for wired Portal authentication users, Portal authentication can still be triggered when a wired Portal authentication user uses HTTP to access a website.

This function takes effect only for new wired Portal authentication users.

Example

Enable HTTPS redirection for wired Portal authentication users.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect wired enable
```

13.5.205 portal logout different-server enable

Function

The **portal logout different-server enable** command configures a device to process user logout requests sent by a Portal server other than the one from which users log in.

The **undo portal logout different-server enable** command restores the default configuration.

By default, a device does not process user logout requests sent by Portal servers other than the one from which users log in.

Format

portal logout different-server enable

undo portal logout different-server enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario where Portal server load balancing is configured, by default, a device does not process user logout requests sent by Portal servers other than the one from which users log in and responds ACK messages only to the Portal server from which users log in. Users in arrears then can still stay online. To prevent this problem, run **portal logout different-server enable** command to configure the device to process user logout requests sent by a Portal server other than the one from which users log in. Upon receipt of a user logout request from such a Portal server, the device starts a user logout process. After completing the logout event, the device responds an ACK message to the Portal server, thereby ensuring that the user logs out properly.

Precautions

The user logout requests that a device can process must be sent by Portal servers bound to an access interface. These servers include all the Portal servers configured in the master and backup Portal server templates bound to the interface.

Example

Enable a device to process user logout requests a Portal server other than the one from which users log in.

```
<HUAWEI> system-view
[HUAWEI] portal logout different-server enable
```

13.5.206 portal logout resend timeout

Function

The **portal logout resend timeout** command configures the re-transmission times and interval for the Portal authentication user logout packet.

The **undo portal logout resend timeout** command restores the default setting.

By default, the Portal authentication user logout packet can be re-transmitted three times within five seconds.

Format

portal logout resend *times* **timeout** *period*

undo portal logout { **resend** | **timeout** } *

Parameters

Parameter	Description	Value
times	Specifies the number of re-transmission times for the Portal authentication user logout packet.	The value is an integer that ranges from 0 to 15. The value 0 indicates that the re-transmission function is disabled.
period	Specifies the re-transmission interval of the Portal authentication user logout packet.	The value is an integer that ranges from 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After disconnecting a Portal authentication user, the device sends a user logout packet (NTF-LOGOUT) to instruct the Portal server to delete the user information. If the network between the device and Portal server is not stable or packets are lost, the Portal server may fail to receive the user logout packet from the device after the Portal authentication user is disconnected. In this case, the user is displayed as disconnected on the device but still as online on the Portal server. To enable the Portal server to receive the user logout packet and ensure that the online user information on the Portal server is correct, the administrator can enable the user logout packet re-transmission function on the device and configure the re-transmission times and interval.

Example

Configure the re-transmission times to 5 and interval to 10 seconds for the Portal authentication user logout packet.

```
<HUAWEI> system-view
[HUAWEI] portal logout resend 5 timeout 10
```

13.5.207 portal max-user

Function

The **portal max-user** command sets the maximum number of concurrent Portal authentication users allowed to access the device.

The **undo portal max-user** command restores the default maximum number of concurrent Portal authentication users.

By default, the number of Portal authentication users is the maximum number of Portal authentication users supported by the device.

Format

portal max-user *user-number*

undo portal max-user

Parameters

Parameter	Description	Value
user-number	Specifies the maximum number of concurrent Portal users.	The value is an integer that varies depending on product models.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **portal max-user** command to set the maximum number of concurrent Portal authentication users.

Example

Set the maximum number of concurrent Portal authentication users to 25.

```
<HUAWEI> system-view
[HUAWEI] portal max-user 25
```

13.5.208 portal pass dns enable

Function

The **portal pass dns enable** command enables a device to allow DNS packets to pass through during Portal authentication.

The **undo portal pass dns enable** command restores the default configuration.

By default, a device does not allow DNS packets to pass through during Portal authentication.

Format

portal pass dns enable

undo portal pass dns enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you use a domain name to access the network, run the **portal pass dns enable** command to allow DNS packets destined for the DNS server to pass through. However, after this command is executed, all DNS packets are permitted.

You are recommended to run the **free-rule** command to configure the IP address of the DNS server as the source accessible to users without authentication.

Example

Enable a device to allow DNS packets to pass through during Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal pass dns enable
```

13.5.209 portal quiet-period

Function

The **portal quiet-period** command enables the quiet timer for Portal authentication.

The **undo portal quiet-period** command disables the quiet timer of Portal authentication.

By default, the quiet timer for Portal authentication is enabled.

Format

portal quiet-period

undo portal quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer for Portal authentication. If the number of Portal authentication failures exceeds the value specified by the **portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. During the quiet period, the device discards Portal authentication requests from the user. This prevents the impact of frequent authentications on the system.

The quiet period for Portal authentication can be set using the **portal timer quiet-period** command. After the quiet period is reached, the device re-authenticates the user.

Example

Enable the quiet timer for Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal quiet-period
```

13.5.210 portal quiet-times

Function

The **portal quiet-times** command sets the maximum number of authentication failures within 60s before a Portal authentication user is kept in quiet state.

The **undo portal quiet-times** command restores the default maximum number of authentication failures within 60s before a Portal authentication user enters the quiet state.

By default, the device allows a maximum of ten authentication failures within 60s before a Portal authentication user enters the quiet state.

Format

portal quiet-times *fail-times*

undo portal quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a Portal authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer, if the number of Portal authentication failures exceeds the value specified by the **portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. This prevents the impact of frequent authentications on the system.

Example

Set the maximum number of Portal authentication failures within 60 seconds to 4.

```
<HUAWEI> system-view
[HUAWEI] portal quiet-times 4
```

13.5.211 portal redirect-302 enable

Function

The **portal redirect-302 enable** command enables redirection based on the status code 302 for Portal authentication.

The **undo portal redirect-302 enable** command disables redirection based on the status code 302 for Portal authentication.

By default, redirection based on the status code 302 is disabled for Portal authentication.

Format

portal redirect-302 enable

undo portal redirect-302 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

HTTP status codes 200 and 302 correspond to different redirection modes. During redirection based on the status code 200 OK, the URL information is in the **URL** field of an HTTP packet. During redirection based on the status code 302, the URL information is in the **Location** field of an HTTP packet. By default, the device performs redirection based on the status code 200 OK. Some applications need to use redirection based on the status code 302. In this case, you can run this command to enable this function.

Precautions

After redirection based on the status code 302 is configured for Portal authentication, the **portal redirect js enable** configuration is invalidated.

Example

Enable redirection based on the status code 302 for Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal redirect-302 enable
```

13.5.212 portal redirect js enable

Function

The **portal redirect js enable** command enables the function of inserting a JavaScript file during Portal redirection.

The **undo portal redirect js enable** command disables the function of inserting a JavaScript file during Portal redirection.

By default, the function of inserting a JavaScript file during Portal redirection is disabled.

Format

portal redirect js enable

undo portal redirect js enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the device redirects the HTTP or HTTPS requests sent from clients to the Portal server. To prevent heavy burdens on the server caused by a large number of HTTP or HTTPS requests sent from the clients and to ensure proper display of the Portal login page, enable the function of inserting a JavaScript file during Portal redirection. After this function is enabled, the HTTP or HTTPS response packets sent from the server carry a JavaScript file. The client browser parses the JavaScript file for redirection, and then performs Portal authentication.

Precautions

The client browser must support and enable the JavaScript function.

Example

Enable the function of inserting a JavaScript file during Portal direction.

```
<HUAWEI> system-view
[HUAWEI] portal redirect js enable
```

13.5.213 portal redirect-http-port

Function

The **portal redirect-http-port** command configures a user-defined destination port number of HTTP packets that trigger Portal redirection.

The **undo portal redirect-http-port** command deletes a user-defined destination port number of HTTP packets that trigger Portal redirection.

By default, the device redirects users to the Portal authentication page only when their browsers send HTTP packets with the destination port number 80.

NOTE

Only the S1720GW-E, S1720GWR-E, S5720-LI, and S5720S-LI support this command.

Format

portal redirect-http-port *port-number* &<1-10>

undo portal redirect-http-port [*port-number* &<1-10>]

Parameters

Parameter	Description	Value
port-number	Specifies a user-defined destination port number of HTTP packets that trigger Portal redirection.	The value is an integer that ranges from 1024 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device redirects users to the Portal authentication page only when their browsers send HTTP packets with the destination port number 80. If a user's browser has a web proxy server configured and the destination port number of HTTP packets is modified, the device discards HTTP packets from the user and does not redirect the user to the Portal authentication page. You can run the **portal redirect-http-port** command to configure a user-defined destination port number of HTTP packets that trigger Portal redirection. The device then redirects users to the Portal authentication page after receiving HTTP packets with the destination port number 80 or a user-defined destination port number.

Precautions

If a user's browser has a web proxy server configured, configure the Portal server address (configured on the device using the **server-ip** command) as an exception address on the user's browser, to prevent HTTP packets to the Portal server from being sent to the web proxy server.

If the specified destination port number is 65535, some browsers consider this port as an insecure port, resulting a redirection failure.

This command applies only when Portal authentication is performed on VLANIF interfaces and does not take effect in other scenarios.

Example

Set the user-defined destination port number to 8080 for HTTP packets that trigger Portal redirection.

```
<HUAWEI> system-view
[HUAWEI] portal redirect-http-port 8080
```


13.5.214 portal timer quiet-period

Function

The **portal timer quiet-period** command configures the quiet period for Portal authentication users who fail to be authenticated.

The **undo portal timer quiet-period** command restores the default quiet period.

By default, the quiet period is 60 seconds for Portal authentication users who fail to be authenticated.

Format

portal timer quiet-period *quiet-period-value*

undo portal timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-value	Sets the quiet period for Portal authentication users who fail to be authenticated.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a Portal authentication user fails to be authenticated consecutively within a short period, the system is affected and a large number of duplicated authentication failure logs are generated.

After the quiet function is enabled using the **portal quiet-period** command, if the number of times that a Portal authentication user fails to be authenticated within 60s exceeds the upper limit (configured using the **portal quiet-times** command), the device discards the user's Portal authentication request packets for a period to avoid frequent authentication failures.

Example

Set the quiet period to 100 seconds for Portal authentication users who fail to be authenticated.


```
<HUAWEI> system-view
[HUAWEI] portal timer quiet-period 100
```

13.5.215 portal timer offline-detect

Function

The **portal timer offline-detect** command sets the Portal user offline detection interval.

The **undo portal timer offline-detect** command restores the default Portal user offline detection interval.

By default, the Portal user offline detection interval is 300 seconds.

Format

portal timer offline-detect *time-length*

undo portal timer offline-detect

Parameters

Parameter	Description	Value
time-length	Specifies the Portal user offline detection interval.	The value is 0 or an integer that ranges from 30 to 7200, in seconds. The default value is 300. The value 0 indicates that offline detection is not performed.

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a Portal user goes offline due to power failure or network interruption, the device and Portal server may still store the user information, which causes incorrect accounting. Additionally, a limit number of users can access the device. If a user goes offline improperly but the device still stores user information, other users cannot access the network.

After the Portal user offline detection interval is set, if the user does not respond within the interval, the device considers the Portal user offline. The device and Portal server then delete the user information and release resources to ensure an efficient resource use.

Precautions

This command only applies to Layer 2 Portal authentication. When the configuration is changed, the new configuration takes effect only for new access users.

The heartbeat detection function of the authentication server can be used to ensure the normal online status of PC users for whom Layer 3 Portal authentication is used. If the authentication server detects that a user goes offline, it instructs the device to disconnect the user.

If the number of offline detection packets (ARP packets) exceeds the default CAR value, the detection fails and the users are logged out (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.). To resolve the problem, the following methods are recommended:

- Increase the detection interval based on the number of users. The default detection interval is recommended when there are less than 8000 users; the detection interval should be no less than 600 seconds when there are more than 8000 users.
- Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

If user traffic (such as service packets) passes through the device within the Portal user offline detection period, the device does not consider the user offline even if the user does not respond to user offline detection packets.

Example

In the Portal access profile **p1**, set the offline detection interval of Portal authentication users to 400s.

```
<HUAWEI> system-view
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] portal timer offline-detect 400
```

13.5.216 portal url-encode enable

Function

The **portal url-encode enable** command enables URL encoding and decoding.

The **undo portal url-encode enable** command disables URL encoding and decoding.

By default, URL encoding and decoding are enabled.

Format

portal url-encode enable

undo portal url-encode enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve web application security, data from untrustworthy sources must be encoded before being sent to clients. URL encoding is most commonly used in web applications. To enable URL encoding and decoding, run the **portal url-encode enable** command. Some special characters in redirect URLs are then converted to secure formats, preventing clients from mistaking them for syntax signs or instructions and unexpectedly modifying the original syntax. In this way, cross-site scripting attacks and injection attacks are prevented.

Precautions

After the URL encoding and decoding function is enabled, some servers may not support the escape characters converted from special characters in redirect URLs. Therefore, check whether servers support the escape characters before configuring special characters in redirect URLs.

Example

Enable URL encoding and decoding.

```
<HUAWEI> system-view
[HUAWEI] portal url-encode enable
```

13.5.217 portal user-alarm percentage

Function

The **portal user-alarm percentage** command sets alarm thresholds for the Portal authentication user count percentage.

The **undo portal user-alarm percentage** command restores the default alarm thresholds for the Portal authentication user count percentage.

By default, the lower alarm threshold for the Portal authentication user count percentage is 50, and the upper alarm threshold for the Portal authentication user count percentage is 100.

Format

portal user-alarm percentage *percent-lower-value percent-upper-value*

undo portal user-alarm percentage

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **portal max-user** command to set the maximum number of online Portal authentication users allowed on a device, you can run the **portal user-alarm percentage** command to set alarm thresholds for the Portal authentication user count percentage.

When the percentage of online Portal authentication users against the maximum number of users allowed by the device exceeds the upper alarm threshold, the device generates an alarm. When the percentage of online Portal authentication users against the maximum number of users allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm.

If the configured upper alarm threshold for the Portal authentication user count percentage is 100, the device generates an alarm when the number of online users reaches the maximum number of users allowed by the device.

Example

Set the lower alarm threshold for the Portal authentication user count percentage to 30, and the upper alarm threshold for the Portal authentication user count percentage to 80.

```
<HUAWEI> system-view
[HUAWEI] portal user-alarm percentage 30 80
```


13.5.218 portal web-authen-server

Function

The **portal web-authen-server** command enables Portal interconnection using the HTTP or HTTPS protocol.

The **undo portal web-authen-server** command disables Portal interconnection using the HTTP or HTTPS protocol.

By default, Portal interconnection using the HTTP or HTTPS protocol is disabled.

Format

portal web-authen-server { **http** | **https ssl-policy** *policy-name* } [**port** *port-number*]

undo portal web-authen-server [**port**]

Parameters

Parameter	Description	Value
http	Configures the HTTP protocol for Portal authentication. **NOTE** The HTTP protocol poses security risks. The HTTPS protocol is recommended.	-
https	Configures the HTTPS protocol for Portal authentication.	-
ssl-policy *policy-name*	Specifies the name of an SSL policy.	The value must be the name of an existing SSL policy.
port *port-number*	Specifies a port number.	The value is an integer that ranges from 1025 to 65535. The default HTTP port number is 8000, and the default HTTPS port number is 8443.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is connected to the Portal server that supports only the HTTP or HTTPS protocol, you need to run the **portal web-authen-server** command on the device to enable Portal interconnection using the HTTP or HTTPS protocol.

Follow-up Procedure

Run the **protocol** command to set the protocol used in Portal authentication to HTTP or HTTPS.

Precautions

- Modifying the **port** parameter will cause users in pre-connection state to go offline.
- In V200R020C10SPC100 and later versions, you must also run the **portal web-authen-server server-source** command to configure the local gateway address used by the device to receive and respond to the packets sent by the user terminals. Otherwise, the Portal interconnection function cannot be used.

Example

Enable Portal interconnection using the HTTPS protocol.

```
<HUAWEI> system-view
[HUAWEI] ssl policy test
[HUAWEI-ssl-policy-test] quit
[HUAWEI] portal web-authen-server https ssl-policy test port 8443
```

13.5.219 portal web-authen-server server-source

Function

The **portal web-authen-server server-source** command configures the local gateway address used by the device to receive and respond to the packets sent by the user terminals when the Portal interconnection function of the HTTP or HTTPS protocol is enabled.

The **undo portal web-authen-server server-source** command restores the default configuration.

By default, the device does not receive or respond to all packets sent by the user terminals when the Portal interconnection function of the HTTP or HTTPS protocol is enabled.

Format

portal web-authen-server server-source { **all-interface** | **ip-address** *ip-address* }

undo portal web-authen-server server-source { **all-interface** | **ip-address** }

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation.
all-interface	Indicates that the IPv4 address is set to 0.0.0.0. That is, the device can receive and respond to all packets sent by the user terminals.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is connected to a Portal server that supports only the HTTP or HTTPS protocol, you need to run the **portal web-authen-server** command on the device to enable the Portal interconnection function of the HTTP or HTTPS protocol. In V200R020C10SPC100 and later versions, you must also run the **portal web-authen-server server-source** command to configure the local gateway address used by the device to receive and respond to the packets sent by the user terminals. Otherwise, the Portal interconnection function cannot be used.

Precautions

- If the system software of the device is upgraded from a version earlier than V200R020C10SPC100 to a later version and the Portal interconnection function of the HTTP or HTTPS protocol is enabled, the device delivers the **portal web-authen-server server-source all-interface** command by default to receive and respond to all packets sent by the user terminals.
- After the **portal web-authen-server server-source all-interface** command is configured, the device receives and responds to all packets sent by the user terminals, which increases system security risks. Therefore, you are not advised to configure this command.
- After the **portal web-authen-server server-source all-interface** command is run, the system clears all configurations of the **portal web-authen-server server-source ip-address** *ip-address* command.
- If the **portal web-authen-server server-source all-interface** command has been configured on the device, the **portal web-authen-server server-source ip-address** *ip-address* command configured later will fail to be delivered.

Example

Configure 10.1.1.1 as the local gateway address used by the device to receive and respond to the packets sent by the user terminals when the Portal interconnection function is enabled.

```
<HUAWEI> system-view
[HUAWEI] portal web-authen-server server-source ip-address 10.1.1.1
```

13.5.220 portal-access-profile (authentication profile view)

Function

The **portal-access-profile** command binds a Portal access profile to an authentication profile.

The **undo portal-access-profile** command unbinds a Portal access profile from an authentication profile.

By default, an authentication profile is not bound to a Portal access profile.

Format

portal-access-profile *access-profile-name*

undo portal-access-profile

Parameters

Parameter	Description	Value
access-profile-name	Specifies the name of a Portal access profile.	The value must be the name of an existing Portal access profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After being bound to a Portal access profile, the authentication profile is enabled with Portal authentication. After the authentication profile is applied to the interface or VAP profile, Portal authentication can be performed on online users.

Prerequisites

The Portal server template used by the Portal access profile has been configured using the **web-auth-server** command.

Follow-up Procedure

Run the **authentication-profile** (Interface view or VAP profile view) command to apply the authentication profile to the interface or VAP profile.

Precautions

An authentication profile can be bound to only one Portal access profile.

If an authentication event authorization VLAN and MAC address, 802.1X, and Portal hybrid authentication are configured in an authentication profile, Portal authentication fails.

If both authentication event authorization VLAN and Portal authentication are configured in an authentication profile, the authentication event authorization VLAN does not take effect.

Example

Bind the authentication profile **portal_authen_profile1** to the Portal access profile **portal_access_profile1**. The IP address of the Portal server is 192.168.10.1, and Layer 2 Portal authentication is used.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server server1
[HUAWEI-web-auth-server-server1] server-ip 192.168.10.1
[HUAWEI-web-auth-server-server1] quit
[HUAWEI] portal-access-profile name portal_access_profile1
[HUAWEI-portal-acces-profile-portal_access_profile1] web-auth-server server1 direct
[HUAWEI-portal-acces-profile-portal_access_profile1] quit
[HUAWEI] authentication-profile name portal_authen_profile1
[HUAWEI-authen-profile-portal_authen_profile1] portal-access-profile portal_access_profile1
```

13.5.221 portal-access-profile (system view)

Function

The **portal-access-profile** command creates a Portal access profile and displays the Portal access profile view.

The **undo portal-access-profile** command deletes the Portal access profile.

By default, the device has a built-in Portal access profile named **portal_access_profile**.

Format

portal-access-profile name *access-profile-name*

undo portal-access-profile name *access-profile-name*

Parameters

Parameter	Description	Value
name *access-profile-name*	Specifies the name of a Portal access profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses Portal access profiles to uniformly manage all Portal users access configurations. To perform Portal authentication for the users in an interface or VAP profile, bind the authentication profile applied to the interface or VAP profile to a Portal access profile.

Follow-up Procedure

Run the **web-auth-server** command to configure the Portal server template for the Portal access profile.

Precautions

- The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in Portal access profile **portal_access_profile** can be modified and applied, but cannot be deleted.
- Before deleting a Portal access profile, ensure that this profile is not bound to any authentication profile.

Example

Create Portal access profile named **portal_access_profile1**.

```
<HUAWEI> system-view
[HUAWEI] portal-access-profile name portal_access_profile1
```


13.5.222 protocol (Portal server template view)

Function

The **protocol** command configures the protocol used in Portal authentication.

The **undo protocol** command restores the default configuration.

By default, the Portal protocol is used in Portal authentication.

Format

protocol { **http** [**password-encrypt** { **none** | **uam** }] | **portal** | **haca** }

undo protocol

Parameters

Parameter	Description	Value
http	Sets the protocol used in Portal authentication to HTTP or HTTPS.	-
password-encrypt { **none** | **uam** }	Specifies the password encoding mode. Select a mode based on the Portal server configuration. ● **none**: The password is not encoded. ● **uam**: The password is encoded using ASCII characters. When **http** is specified, the default password encoding mode is **none**.	-
portal	Sets the protocol used in Portal authentication to Portal.	-
haca	Sets the protocol used in Portal authentication to HACA.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

In Portal authentication, the device can use the following protocols to communicate with the Portal server. You can set the protocol according to the protocol supported by the Portal server.

- HACA protocol
- Portal protocol
- HTTP or HTTPS protocol

Central cloud APs do not support HTTP or HTTPS for Portal authentication.

Example

According to the Portal server configuration, set the protocol used in Portal authentication to HTTP or HTTPS and set the password encryption mode to **uam** on the device.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] protocol http password-encrypt uam
```

13.5.223 qos-profile (service scheme view)

Function

The **qos-profile** command binds a QoS profile to a service scheme.

The **undo qos-profile** command unbinds the QoS profile from the service scheme.

By default, no QoS profile is bound to a service scheme.

NOTE

Only S5731-H,S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

qos-profile *profile-name*

undo qos-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the QoS profile bound to the service scheme.	The value must be the name of an existing QoS profile.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme (AAA view)** command, you can run the **qos-profile** command to bind a QoS profile to the service scheme. The user assigned with the service scheme will have the attributes in the QoS profile.

Precautions

For S6720-EI, S6720S-EI, if the user upstream rate limit is configured in the QoS profile bound to a service scheme, do not configure the device to use the service scheme to grant network access rights to users in the pre-connection phase. Otherwise, users go offline.

If the server delivers both the downlink bandwidth limit (equivalent to the RADIUS attribute HW-Output-Committed-Information-Rate) and the RADIUS attribute HW-Subscriber-QoS-Profile for user authorization, only the RADIUS attribute HW-Subscriber-QoS-Profile takes effect.

If the server delivers both the uplink or downlink bandwidth limit (equivalent to the RADIUS attribute HW-Input-Committed-Information-Rate or HW-Output-Committed-Information-Rate) and the RADIUS attribute HW-Qos-Data for user authorization, only the uplink or downlink bandwidth limit take effect.

Example

Bind the QoS profile **abc** to the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name abc
[HUAWEI-qos-abc] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] qos-profile abc
```

13.5.224 reset aaa statistics access-type-authenreq

Function

The **reset aaa statistics access-type-authenreq** command clears the number of requesting for MAC, Portal, or 802.1X authentication.

Format

reset aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, and 802.1X authentications.

To clear the number of requesting for MAC, Portal, or 802.1X authentication, run the **reset aaa statistics access-type-authenreq** command.

Example

Clear the number of requesting for MAC, Portal, or 802.1X authentication.

```
<HUAWEI> reset aaa statistics access-type-authenreq
```

13.5.225 reset access-user dot1x-identity statistics

Function

The **reset access-user dot1x-identity statistics** command clears statistics about Identity packets for 802.1X authentication on a switch.

Format

reset access-user dot1x-identity statistics

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To display statistics about Identity packets for 802.1X authentication on a switch within a specified period of time, run the **reset access-user dot1x-identity**

statistics command to clear the existing statistics first, and then run the **display access-user dot1x-identity statistics** command to display the new statistics.

Example

Clear statistics about Identity packets for 802.1X authentication on the switch.

```
<HUAWEI> system-view
[HUAWEI] reset access-user dot1x-identity statistics
```

13.5.226 reset access-user https statistics

Function

The **reset access-user https statistics** command clears statistics about HTTPS protocol packets sent to the CPU.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

reset access-user https statistics

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Before checking statistics about HTTPS protocol packets sent to the CPU within a specified period, you must run the **reset access-user https statistics** command to clear the existing statistics. After new statistics are collected, run the **display access-user https statistics** command to check the new statistics.

Example

Clear statistics about HTTPS protocol packets sent to the CPU.

```
<HUAWEI> system-view
[HUAWEI] reset access-user https statistics
```


13.5.227 reset access-user portal statistics

Function

The **reset access-user portal statistics** command clears statistics about Portal protocol packets sent to the CPU.

Format

reset access-user portal statistics

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Before checking statistics about Portal protocol packets sent to the CPU within a specified period, you must run the **reset access-user portal statistics** command to clear the existing statistics. After new statistics are collected, run the **display access-user portal statistics** command to check the new statistics.

Example

Clear statistics about Portal protocol packets sent to the CPU.

```
<HUAWEI> system-view
[HUAWEI] reset access-user portal statistics
```

13.5.228 reset access-user traffic-statistics

Function

The **reset access-user traffic-statistics** command clears statistics on traffic of users.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

reset access-user traffic-statistics { **user-id** *begin-id* [*end-id*] | **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance*] }

Parameters

Parameter	Description	Value
user-id *begin-id* [*end-id*]	Specifies IDs of online users. • *begin-id*: indicates the ID of the start user. • *end-id*: indicates the ID of the end user. The value of *end-id* must be equal to or greater than that of *begin-id*.	The value is an integer that varies depending on the product model.
mac-address *mac-address*	Specifies the MAC address of an online user.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits.
ip-address *ip-address*	Specifies the IP address of an online user.	The value is in dotted decimal notation.
vpn-instance *vpn-instance*	Specifies the name of a VPN instance that an online user belongs to.	The value must be an existing VPN instance name.

Views

User view

Default Level

3: Management level

Usage Guidelines

After traffic policing is configured in a service scheme, the device collects traffic statistics for the users assigned with the service scheme. You can run the **reset access-user traffic-statistics** command to clear traffic statistics of online users.

Example

Clear statistics on traffic of the user with the IP address 10.1.1.1.

```
<HUAWEI> reset access-user traffic-statistics ip-address 10.1.1.1
```

13.5.229 reset dot1x statistics

Function

The **reset dot1x statistics** command clears 802.1X authentication statistics.

Format

reset dot1x statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears 802.1X authentication statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, 802.1X authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The 802.1X authentication statistics contain the number of times that the authentication succeeded and failed and the number of sent and received packets.

The **reset dot1x statistics** command is used in the following scenarios:

- Redeploy services. After the statistics are cleared, collect the 802.1X authentication statistics again, and run the **display dot1x** command to check whether the authentication function works properly and whether packets are correctly sent and received.
- Rectify a fault. After the fault is rectified, run the **reset dot1x statistics** command to clear the statistics, collect the statistics on 802.1X authentication again, and then run the **display dot1x** command to verify the authentication result and check whether packets are correctly sent and received. If the authentication is successful and packets are correctly sent and received, the fault is rectified.

Example

Clear 802.1X authentication statistics.

```
<HUAWEI> reset dot1x statistics
```

13.5.230 reset dot1x-client statistics

Function

The **reset dot1x-client statistics** command clears packet statistics about 802.1X clients.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

reset dot1x-client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears packet statistics about the 802.1X client on a specified interface. If this parameter is not specified, packet statistics about 802.1X clients on all interfaces are cleared.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to clear packet statistics about 802.1X clients, and then run the **display dot1x-client statistics** command to view the new statistics.

Example

Clear packet statistics about 802.1X clients.

<HUAWEI> **reset dot1x-client statistics**

13.5.231 reset mac-authen statistics

Function

The **reset mac-authen statistics** command clears MAC address authentication statistics.

Format

reset mac-authen statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears MAC address authentication statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, MAC address authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset mac-authen statistics** command is used in the following scenarios:

- Re-deploy services. After the statistics are cleared, collect the MAC address authentication statistics again, and run the **display mac-authen** command to check whether the authentication function is normal.
- Rectify a fault. After the fault is rectified, run the **reset mac-authen statistics** command to clear statistics, collect MAC address authentication statistics

again, and run the **display mac-authen** command to check the authentication result. If the authentication is successful, the fault is rectified.

Example

Clear MAC address authentication statistics.

```
<HUAWEI> reset mac-authen statistics
```

13.5.232 rule (terminal type identification profile view)

Function

The **rule** command configures a terminal type identification rule.

The **undo rule** command deletes a terminal type identification rule.

By default, a terminal type identification rule is not configured.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

rule *rule-id* { **mac** *mac-address* **mask** { *mask-length* | *mask* } | **dhcp-option** *option-id* { **sub-match** | **all-match** } { **ascii** *option-text* | **hex** *option-hex-string* } | **user-agent** { **sub-match** | **all-match** } *user-agent-text* }

undo rule *rule-id*

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of a terminal type identification rule.	The value is an integer that ranges from 0 to 7.
mac *mac-address*	Specifies a terminal MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
mask { *mask-length* | *mask* }	Indicates the mask or mask length of a terminal MAC address.	The value of *mask* is in H-H-H format. An H is a hexadecimal number of 4 digits. The value of *mask-length* is an integer that ranges from 1 to 48.

Parameter	Description	Value
dhcp-option *option-id*	Identifies the terminal type using a DHCP option. *option-id* specifies the ID of a DHCP option.	The value is an integer that ranges from 1 to 254. **NOTE** Currently, the identification rule takes effect only when the value is set to 12, 55, or 60.
sub-match	Indicates partial match. The user agent (UA) or Option information detected by the AC must be the same as or contain the value of *option-text* or *user-agent-text*.	-
all-match	Indicates exact match. The UA or Option information detected by the AC must be the same as the value of *option-text* or *user-agent-text*.	-
ascii *option-text*	Specifies the Option information that a terminal must match as an ASCII string.	The value is a string of 1 to 247 case-sensitive characters, spaces supported.
hex *option-hex-string*	Specifies the Option information that a terminal must match as a hexadecimal string.	The value is a string of 1 to 254 case-insensitive characters without spaces and supports only digits and letters (A to F or a to f).
user-agent	Identifies the terminal type using UA information.	-
user-agent-text	Specifies the UA information that a terminal must match.	The value is a string of 1 to 247 case-sensitive characters.

Views

Terminal type identification profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A terminal type identification rule is set based on the terminal's MAC address, UA, and DHCP Option information.

- Match the first 24 bits of a terminal's MAC address, which is known as the Organizationally Unique Identifier (OUI), to identify the corresponding manufacturer.
- Use the UA information carried in HTTP packets from a terminal to identify the operating system and its version, the CPU type, browser type, and browser version.
- Use the manufacturer information carried in Option12, Option55, and Option60 in DHCP packets from a terminal to identify the terminal's host name and manufacturer type.

A terminal type can be identified by checking whether the terminal information matches the identification rule configured. Once the identification is performed, user rights can be delivered or access control can be implemented based on terminal types.

Precautions

- To match an identification rule, the terminal information must be the same as all the configuration items in the rule.
- If the specified *rule-id* already exists and the new rule conflicts with the original rule, the new rule replaces the original one in the conflicting part, which is the same as editing an existing rule.
- To modify a rule that already contains *rule-id*, delete the old rule and create a rule. Otherwise, the configuration result may be incorrect.
- When a terminal's information meets conditions of identification rules in multiple terminal type identification profiles, the terminal type identification profile that contains MAC address-based identification rules is preferentially matched.

Example

Configure terminal type identification rule 1 in the terminal type identification profile **test**.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
[HUAWEI-device-profile-test] rule 1 mac 00e0-fc59-1ee0 mask 12
```

13.5.233 remote-access-user manage

Function

The **remote-access-user manage** command enables user management through Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS).

The **undo remote-access-user manage** command disables HTTP- or HTTPS-based user management.

By default, HTTP- or HTTPS-based user management is disabled.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

remote-access-user manage { **http** | **https ssl-policy** *policy-name* } **port** *port-num* [**acl** *acl-number*]

undo remote-access-user manage { **http** | **https ssl-policy** *policy-name* } **port** *port-num* [**acl** *acl-number*]

Parameters

Parameter	Description	Value
http	Specifies HTTP-based user management.	-
https	Specifies HTTPS-based user management.	-
ssl-policy *policy-name*	Specifies the SSL policy used by the built-in Portal server.	The value must be the name of an existing SSL policy. The SSL policy type must be set to server SSL policy.
port *port-num*	Specifies a port number.	• For HTTP, the value can be 80 or any integer in the range of 1025 to 55535. • For HTTPS, the value can be 443 or any integer in the range of 1025 to 55535.
acl *acl-number*	Specifies the number of an ACL.	The value is an integer in the range from 3000 to 3999 and must be an existing ACL number. **NOTE** A maximum of 64 ACLs can be delivered. If more than 64 ACLs are configured, only the first 64 ACLs take effect.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **remote-access-user manage** command is run, you can manage access users through HTTP or HTTPS on a remote host or server, including forcibly logging out users and deregistering users (by modifying the user status to pre-connection). You can also configure an ACL in the command to specify which remote hosts or servers can be used to manage users.

Prerequisites

Before enabling HTTPS-based user management, run the **ssl policy** *policy-name* command in the system view to create an SSL policy.

Precautions

- If an ACL is specified, the source IP addresses defined in the ACL rules must use service ports, instead of management ports, to communicate with the device.
- In V200R020C10SPC100 and later versions, after HTTP- or HTTPS-based user management is enabled, you must also run the **remote-access-user manage server-source** command to configure the local gateway address used by the device to receive and respond to packets. Otherwise, HTTP- or HTTPS-based user management cannot be used.

Example

Enable HTTP-based user management.

```
<HUAWEI> system-view
[HUAWEI] remote-access-user manage http port 8080
```

13.5.234 remote-access-user manage server-source

Function

The **remote-access-user manage server-source** command configures the local gateway address used by the device to receive and respond to packets when HTTP- or HTTPS-based user management is enabled.

The **undo remote-access-user manage server-source** command restores the default configuration.

By default, the device does not receive or respond to any packets when HTTP- or HTTPS-based user management is enabled.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

remote-access-user manage server-source { **all-interface** | **ip-address** *ip-address* }

undo remote-access-user manage server-source { **all-interface** | **ip-address** }

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation.
all-interface	Indicates that the IPv4 address is set to 0.0.0.0. That is, the local gateway address used by the device to receive and respond to packets can be any address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In V200R020C10SPC100 and later versions, after HTTP- or HTTPS-based user management is enabled, you must also run the **remote-access-user manage server-source** command to configure the local gateway address used by the device to receive and respond to packets. Otherwise, HTTP- or HTTPS-based user management cannot be used.

Precautions

- If the system software of the device is upgraded from a version earlier than V200R020C10SPC100 to a later version and HTTP- or HTTPS-based user management is enabled, the device delivers the **remote-access-user manage server-source all-interface** command by default to set the local gateway address used by the device to receive and respond to packets to any address.
- After the **remote-access-user manage server-source all-interface** command is configured, the local gateway address used by the device to receive and respond to packets can be any address, which increases system security risks. Therefore, you are not advised to configure this command.

- After the **remote-access-user manage server-source all-interface** command is run, the system clears all configurations of the **remote-access-user manage server-source ip-address** *ip-address* command.
- If the **remote-access-user manage server-source all-interface** command has been configured on the device, the **remote-access-user manage server-source ip-address** *ip-address* command configured later will fail to be delivered.

Example

Configure 10.1.1.1 as the local gateway address for user management.

```
<HUAWEI> system-view
[HUAWEI] remote-access-user manage server-source ip-address 10.1.1.1
```

13.5.235 server-detect

Function

The **server-detect** command enables the Portal server detection function.

The **undo server-detect** command disables the Portal server detection function.

By default, the Portal server detection function is disabled.

Format

server-detect [**interval** *interval-period* | **max-times** *times* | **critical-num** *critical-num* | **action** { **log** | **trap** } *] *

undo server-detect [**interval** | **max-times** | **critical-num** | **action** { **log** | **trap** } *]

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the detection interval of the Portal server.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 60.
max-times *times*	Specifies the maximum number of times that the detection fails.	The value is an integer that ranges from 1 to 255. The default value is 3.
critical-num *critical-num*	Specifies the minimum number of Portal servers in Up state.	The value is an integer that ranges from 0 to 128. The default value is 0. The default value is recommended.

Parameter	Description	Value
action	Specifies the action to be taken after the number of detection failures exceeds the maximum.	-
log	Indicates that the device sends a log after the number of detection failures exceeds the maximum.	-
trap	Indicates that the device sends a trap after the number of detection failures exceeds the maximum.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

If the communication is interrupted because the network between the device and Portal server is faulty or the Portal server is faulty, new Portal authentication users cannot go online. This brings great inconvenience to users.

After the Portal server detection function is enabled in the Portal server template, the device detects all Portal servers configured in the Portal server template. If the number of times that the device fails to detect a Portal server exceeds the upper limit, the status of the Portal server is changed from Up to Down. If the number of Portal servers in Up state is less than or equal to the minimum number (specified by the **critical-num** parameter), the device performs the corresponding operation to allow the administrator to obtain the real-time Portal server status or ensure that the users have certain network access rights.

NOTE

The detection interval of the Portal server multiplied by the maximum number of detection failures cannot be less than the keepalive heartbeat interval of the Portal server. It is recommended that the configured detection interval of the Portal server be greater than the keepalive heartbeat interval of the Portal server.

The device does not support IPv6 Portal server detection.

If the Portal server does not support detection, you do not need to configure this command.

- You are advised to use the default value of the **critical-num** parameter for the following reasons:
  - If the number of Portal servers in Up state is less than or equal to the value of **critical-num**, the value of **Status** in the **display server-detect state** command output is **Abnormal**. If the authentication escape function is configured, users are granted limited network access rights.
  - If the number of Portal servers in Up state is greater than the value of **critical-num**, the value of **Status** in the **display server-detect state** command output is **Normal**.
  - If there is only one Portal server and **critical-num** is set to 1, the number of Portal servers in Up state is equal to the value of **critical-num** when the Portal server goes Up. In this case, the value of **Status** in the **display server-detect state** command output is **Abnormal**. In such scenarios, you need to set **critical-num** to the default value **0** so that the value of **Status** is **Normal**.

Example

Enable the Portal server detection and keepalive function in the Portal server template **abc**, set the detection interval to 100s, set the maximum number of failures to 5, and specify the log sent after the number of failures exceeds the limit.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] server-detect interval 100 max-times 5 action log
```

13.5.236 server-detect type

Function

The **server-detect type** command configures the mode in which a device detects Portal server status.

The **undo server-detect type** command restores the default Portal server detection mode.

By default, the Portal-based Portal server detection mode is configured.

Format

server-detect type { **portal** | **http** }

undo server-detect type

Parameters

Parameter	Description	Value
portal	Specifies the Portal-based Portal server detection mode.	-
http	Specifies the HTTP-based Portal server detection mode.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Precautions

In Portal-based Portal server detection mode, the Portal server periodically (the time is determined by the server) sends heartbeat packets to the access device, which then determines the server reachability based on the heartbeat packets. If the access device receives Portal heartbeat packets or other authentication packets from the Portal server within the detection interval (configured using **server-detect interval** *interval-period*) and the packets are verified to be correct, the detection is successful. Otherwise, the detection fails. When the number of consecutive detection failures reaches the maximum number specified by the **server-detect max-times** *times* command, the access device changes the status of the Portal server from Up to Down.

In HTTP-based Portal server detection mode, the access device periodically sends HTTP packets to the Portal server and expects a response packet from the Portal server. If the access device receives a response packet within the specified detection interval (configured using **server-detect interval** *interval-period*), the detection is successful. Otherwise, the detection fails. When the number of consecutive detection failures reaches the maximum number specified by the **server-detect max-times** *times* command, the access device changes the status of the Portal server from Up to Down.

In Portal-based Portal server detection mode, the Portal server must use the Portal protocol and support sending Portal heartbeat packets. If the Portal server does not meet these requirements, you can configure the HTTP-based detection mode. In this way, if the device detects that the Portal server is Down, the device grants new users the corresponding network access rights.

Precautions

HTTP-based Portal server detection applies to both wireless access scenarios and wired access scenarios using MAC+Portal authentication.

Example

Configure the device to detect Portal server status using HTTP.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] server-detect type http
```

13.5.237 server-ip (Portal server template view)

Function

The **server-ip** command configures an IP address for a Portal server.

The **undo server-ip** command deletes an IP address for a Portal server.

By default, no IP address is configured for a Portal server.

Format

server-ip *server-ip-address* &<1-10>

server-ip ipv6 *server-ipv6-address* &<1-3>

undo server-ip { *server-ip-address* | **all** }

undo server-ip ipv6 { *server-ipv6-address* | **all** }

NOTE

The **ipv6** *server-ipv6-address* parameter is only supported by the following models:

S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S500, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720-EI, S6720S-EI

Parameters

Parameter	Description	Value
server-ip-address	Specifies an IPv4 address of a Portal server.	The value is in dotted decimal notation.
ipv6 *server-ipv6-address*	Specifies an IPv6 address of a Portal server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
all	Deletes all IPv4 addresses of a Portal server.	-
ipv6 all	Deletes all IPv6 addresses of a Portal server.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server template on the device using the **web-auth-server (system view)** command, configure parameters for the template.

Run the **server-ip** command to configure an IP address for the Portal server in the Portal server template view. When receiving a Portal authentication request packet from a user, the device sends a response packet to the Portal server with the configured IP address. Multiple IP addresses can be configured in a Portal server template. This configuration allows Portal authentication users to access the same Portal authentication page using multiple IP addresses, making the authentication process more flexible.

Precautions

- After the IP address corresponding to a Portal server is configured in the Portal server template, users are allowed to access the IP address. If the destination URL in an HTTP packet matches this IP address, redirection is not triggered.
- If multiple IP addresses are configured for a Portal server in the Portal server template, you are advised to run the **url (Portal server template view)** command to configure a URL for the Portal server. If no URL is configured, the device uses the first IP address as the URL by default, and the other IP addresses do not take effect. When the switch functions as the AC, configured server IP addresses will be automatically delivered to APs and authentication-free rules will be generated. Currently, only the first four IPv4 addresses and the first four IPv6 addresses take effect on the APs.
- When you run the **server-ip** command to specify IPv6 addresses, you must also specify IPv4 addresses. This is because the device does not support IPv6 Portal protocol exchange.

Example

Set the Portal server IP address in the Portal server template **test** to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] server-ip 10.10.10.1
```


13.5.238 server-source (Portal server template view)

Function

The **server-source** command configures the local gateway address used by the device to receive and respond to the packets sent by the Portal server when Portal authentication is enabled.

The **undo server-source** command restores the default configuration.

By default, the device does not receive any packets from the Portal server.

Format

server-source ip-address *ip-address*

undo server-source ip-address

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

V200R020C10SPC100 and later versions: If Portal authentication is enabled on the device, you must configure the local gateway address used by the device to receive and respond to the packets sent by the Portal server. You can use either of the following methods to configure the address:

- Run the **web-auth-server server-source all-interface** command in the system view.
- Run the **server-source ip-address** *ip-address* command in the Portal server template view.

Precautions

- If the system software of the device is upgraded from a version earlier than V200R020C10SPC100 to a later version and Portal authentication is enabled, the device delivers the **web-auth-server server-source all-interface** command by default.

- After the **web-auth-server server-source all-interface** command is run, the system clears all configurations of the **server-source ip-address** *ip-address* command.
- If the **web-auth-server server-source all-interface** command has been configured on the device, the **server-source ip-address** *ip-address* command configured later will fail to be delivered.

Example

In the Portal server template **server1**, configure 10.1.1.1 as the local gateway address used by the device to receive and respond to the packets sent by the Portal server.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server server1
[HUAWEI-web-auth-server-server1] server-source ip-address 10.1.1.1
```

13.5.239 shared-key (Portal server template view)

Function

The **shared-key** command configures the shared key that the device uses to exchange information with a Portal server.

The **undo shared-key** command restores the default setting.

By default, no shared key that the device uses to exchange information with a Portal server is configured.

Format

shared-key cipher *key-string*

undo shared-key

Parameters

Parameter	Description	Value
cipher	Displays a shared key in cipher text.	-
key-string	Specifies the shared key.	The value is a string of case-sensitive characters without spaces. It can be a string of 1 to 255 characters in plain text, or a string of 20 to 392 characters in cipher text. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a shared key is configured using the **shared-key** command, the Portal packet exchanged between the device and Portal server carries an authenticator generated according to the shared key, and the authenticator is used to check whether the Portal packet at the receiver is correct. This effectively improves the information exchange security.

Precautions

To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 16 characters.

Example

Configure the shared key in the Portal server template **test** to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] shared-key cipher YsHsjx_202206
```

13.5.240 source-ip (Portal server template view)

Function

The **source-ip** command configures the source IP address for the device to communicate with a Portal server.

The **undo source-ip** command restores the default setting.

By default, no source IP address is configured for the device to communicate with a Portal server.

Format

source-ip *ip-address*

undo source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for communication with a Portal server.	The value is in dotted decimal notation.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure normal communication between the device and Portal server, run the **source-ip** command to configure a source IP address on the device.

If the device is configured with a loopback IP address and a common IP address, the device can communicate with the Portal server only when the loopback IP address and common IP address are the same. The **source-ip** command configures a source IP address on the device in the Portal server template view to allow communication between the device and a Portal server.

Precautions

Ensure that the configured source IP address is the device IP address. The source IP address cannot be 255.255.255.255, all 0s, class D address, class E address, or loopback address.

Example

Set the source IP address for communication between the device and a Portal server to 192.168.1.100 in the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] source-ip 192.168.1.100
```

13.5.241 source-interface (Portal server template view)

Function

The **source-interface** command configures an IP address of a specified interface as the source IP address used by the device to communicate with the Portal server.

The **undo source interface** command restores the default configuration.

By default, no source IP address is configured for the device.

Format

source-interface *interface-type interface-number*

undo source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Configures an IP address of a specified interface as the source IP address used by the device to communicate with the Portal server: • *interface-type* specifies the interface type. **NOTE** The interface must be a loopback interface. • *interface-number* specifies the interface number.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to communicate with the Portal server normally, ensure that the source IP address in the packets sent by the device to the Portal server is consistent with the device IP address configured on the Portal server. By default, the device uses the IP address of an outbound interface as the source IP address to communicate with the Portal server. When there are multiple outbound interfaces and the outbound interface sending packets changes, the source IP address in the packets sent by the device to the Portal server becomes inconsistent with the device IP address configured on the Portal server. In this situation, communication between the device and Portal server is interrupted. To address this problem, run the **source-interface** command on the device to specify the IP address of a loopback interface as the source IP address used by the device to communicate with the Portal server.

Precautions

The specified interface must be a Layer 3 interface with an IP address configured.

Example

Configure an IP address of a specified interface as the source IP address used by the device to communicate with the Portal server.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] ip address 10.1.2.25 24
[HUAWEI-LoopBack1] quit
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] source-interface loopback 1
```


13.5.242 static-user

Function

The **static-user** command configures a static user.

The **undo static-user** command deletes the configured static user.

By default, no static user is configured.

Format

static-user *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*] [**ip-user**] [**domain-name** *domain-name* | **interface** *interface-type interface-number* [**detect**] | **mac-address** *mac-address* | **vlan** *vlan-id* | **keep-online**] *

undo static-user *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
start-ip-address [*end-ip-address*]	Specifies the IP address range to which a static user belongs. If *end-ip-address* is not specified, the static user is specified by *start-ip-address*.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance to which a static user belongs.	The value must be an existing VPN instance name.
ip-user	Identifies a static user using an IP address. **NOTE** This parameter is only supported by the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.	-

Parameter	Description	Value
domain-name *domain-name*	Specifies the domain to which a static user belongs. If this parameter is specified, the user name of the static user is in the format of user name@domain name. In this case, @ is the default domain name delimiter. The location of delimiter and domain name can be set as required.	The value must be an existing domain name.
interface *interface-type interface-number*	Specifies the interface connected to a static user. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** A management interface cannot be configured as the interface to which a static user belongs.	-
detect	Permits the device to send ARP packets to trigger MAC address authentication for offline static users.	-
mac-address *mac-address*	Specifies the MAC address for a static user.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits.
vlan *vlan-id*	Specifies the VLAN to which a static user belongs.	The value is an integer that ranges from 1 to 4094.
keep-online	Keeps a static user online, with offline detection not performed.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In network deployment, static IP addresses are assigned to dumb terminals such as printers and servers. These users can be configured as static users for flexible authentication.

After static users are configured, the device can use static user information such as their IP addresses as the user names to authenticate the users only if one of the 802.1X authentication, MAC address authentication, and Portal authentication modes is enabled on the interfaces connected to the static users.

When **ip-user** is specified, IP addresses are used to identify static users and control their permission.

- When some terminals have multiple IP addresses and one MAC address, and they can access the network only after each IP address is authenticated, specify the **ip-user** parameter to identify these users and configure the **ip-static-user enable** command in the authentication template bound to the user access interfaces.
- When all terminals have multiple IP addresses and can access the network only after each IP address is authenticated, only configure the **ip-static-user enable** command in the authentication template bound to the user access interfaces.

Precautions

If a **static-user** command with **ip-user** specified is configured, other **static-user** command configurations without **ip-user** specified become invalid. To enable the **static-user** commands without **ip-user** to take effect, cancel the **static-user** command configuration with **ip-user**, or specify **ip-user** in all **static-user** commands.

After the **static-user** command is executed to modify the configuration, if a new user cannot log in due to an IP address conflict with an existing user, you need to run the **cut access-user** command to force the existing user to log out.

When the interface (**interface** *interface-type interface-number*) mapping static users is specified, the VLAN (**vlan** *vlan-id*) to which the interface belongs must be configured.

This function takes effect only for users who go online after this function is successfully configured.

Only when static users have the **ip-user** parameter configured and connect to the interfaces bound to the authentication template in which the **ip-static-user enable** command configured, IP addresses can be used to identify these users and control their permission.

After this command is configured to specify the VLAN to which a static user belongs, and the user is authenticated and the VLAN is authorized, if the authorized VLAN is different from the previously specified VLAN, the user is added to the new authorized VLAN and is no longer a static user.

When the command is configured on the UC device and directly delivered to the ASs in the SVF scenario, the command must be in the following format: **static-user** *start-ip-address* [*end-ip-address*] { **vlan** *vlan-id* | **mac-address** *mac-address* } or **static-user** *start-ip-address* [*end-ip-address*] **vlan** *vlan-id* **mac-address** *mac-address*.

In SVF mode, when the **direct-command view command static-user** command is executed on the control device to deliver the static-user configuration to access devices, the configuration must be the same as the **static-user** command configuration on the control device. If they are different, the **static-user** command configuration on the control device takes effect.

In policy association scenarios, the **static-user** command is optional on access devices. When this command is configured, the static-user configuration must be the same as that on the control device. If they are different, the **static-user** command configuration on the control device takes effect.

Example

Configure the IP address range of 10.1.1.1 to 10.1.1.10, authentication domain **test**, and VLAN 10 for static users.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] quit
[HUAWEI-aaa] quit
[HUAWEI] static-user 10.1.1.1 10.1.1.10 domain-name test vlan 10
```

13.5.243 static-user not-update-ip enable

Function

The **static-user not-update-ip enable** command disables the device from updating IP addresses of static users.

The **undo static-user not-update-ip enable** command allows the device to update IP addresses of static users.

By default, the device cannot update IP addresses of static users.

Format

static-user not-update-ip enable

undo static-user not-update-ip enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IP addresses for static users are configured, terminals using these IP addresses are authenticated as static users. After these terminals go online, they may send abnormal ARP packets whose source IP addresses are not the IP addresses of static users to the authentication device. After receiving the packets, the device updates terminal IP addresses in CIB entries. As a result, the terminals are no longer static users and go offline. To prevent this problem, you can run the **static-user not-update-ip enable** command to disable the device from updating IP addresses of static users.

Precautions

When the **undo static-user not-update-ip enable** command is configured and the function of identifying static users through IP addresses is enabled, only the function of identifying static users through IP addresses takes effect.

Example

Disable the device from updating IP addresses of static users.

```
<HUAWEI> system-view
[HUAWEI] static-user not-update-ip enable
```

13.5.244 static-user password

Function

The **static-user password** command sets the password for a static user in authentication.

The **undo static-user password** command restores the default password for the static user.

By default, the password for a static user in authentication not set.

Format

static-user password cipher *password*

undo static-user password

Parameters

Parameter	Description	Value
cipher	Indicates that the password is displayed in cipher text.	-
password	Specifies the password of a static user.	The value is a case-sensitive string without question marks (?) or spaces. The password contains 1 to 128 characters in plain text or 48 to 188 characters in cipher text. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a static user triggers authentication through an ARP packet, you can run the **static-user password** command to set the password for the static user. The access device then sends the password to the authentication server.

Precautions

To improve security, change the default password immediately and update the password periodically. It is recommended that the new password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

This function takes effect only for users who go online after this function is successfully configured.

Example

Set YsHsjx_202206 as the static user password for authentication.

```
<HUAWEI> system-view
[HUAWEI] static-user password cipher YsHsjx_202206
```


13.5.245 static-user username format-include

Function

The **static-user username format-include** command sets the user name for a static user in authentication.

The **undo static-user username format-include** command restores the default user name for the static user.

By default, the name of a static user consists of **system-name** and **ip-address**. For example, if the access device name is **test** and user IP address is 1.1.1.1, the static user name is **test1.1.1.1**.

Format

static-user username format-include { **ip-address** | **mac-address** | **system-name** }

undo static-user username format-include

Parameters

Parameter	Description	Value
ip-address	Specifies the user IP address as the static user name.	-
mac-address	Specifies the user MAC address as the static user name.	-
system-name	Specifies the access device name as the static user name. To configure the device name, run the **sysname** command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a static user triggers authentication through an ARP packet, you can run the **static-user username format-include** command to set the user name for the

static user. The access device then sends the user name to the authentication server.

NOTE

If the user name of a static user contains a device name whose length exceeds 16 bytes, the system uses only the first 16 bytes of the device name.

This function takes effect only for users who go online after this function is successfully configured.

Example

Set the user IP address as the static user name for authentication.

```
<HUAWEI> system-view
[HUAWEI] static-user username format-include ip-address
```

13.5.246 static-user username macaddress format

Function

The **static-user username macaddress format** command sets the user name for authenticating a static user to a MAC address.

The **undo static-user username macaddress format** command restores the default setting.

By default, the user name for authenticating a static user is not set to a MAC address.

Format

static-user username macaddress format { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password-with-macaddress**]

undo static-user username macaddress format

Parameters

Parameter	Description	Value
with-hyphen [**normal**] [**colon**] | **without-hyphen**	Specifies the format of a MAC address. • **with-hyphen**: indicates that the MAC address contains hyphens (-), for example, 00e0-fc12-3456. • **with-hyphen normal**: indicates that the MAC address contains hyphens (-), for example, 00-e0-fc-12-34-56. • **with-hyphen colon**: indicates that the MAC address contains colons (:), for example, 00e0:fc12:3456. • **with-hyphen normal colon**: indicates that the MAC address contains colons (:), for example, 00:e0:fc:12:34:56. • **without-hyphen**: indicates that the MAC address does not contain hyphens (-) or colons (:), for example, 00e0fc123456.	-
uppercase	Configures a MAC address in uppercase format as the user name for authentication. If this parameter is not specified, a MAC address in lowercase format is used.	-

Parameter	Description	Value
password-with-macaddress	Configures a MAC address as the password. If this parameter is not specified, the password configured in the **static-user password cipher** *password* command is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In network deployment, static IP addresses are assigned to dumb terminals such as printers, that is, their users are configured as static users. To authenticate a static user, you can run this command to set the user name and password for authentication to a MAC address. This command takes priority over the **static-user username format-include** { **ip-address** | **mac-address** | **system-name** } command and **static-user password cipher** *password* command.

Example

Set the MAC address with hyphens (-) as the user name and password for authenticating a static user.

```
<HUAWEI> system-view
[HUAWEI] static-user username macaddress format with-hyphen password-with-macaddress
```

13.5.247 traffic-filter acl

Function

The **traffic-filter acl** command configures ACL-based packet filtering.

The **undo traffic-filter acl** command deletes the ACL configured for packet filtering.

By default, ACL-based packet filtering is not configured.

Format

traffic-filter inbound acl [**ipv6**] { *acl-number* | **name** *acl-name* }

undo traffic-filter inbound acl [**ipv6**] { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures packet filtering in the inbound direction of the interface.	-
acl-number	Specifies the ID of the user ACL or user ACL6 configured for packet filtering.	The value is an integer in the range from 6000 to 9999. If the configured user ACL or user ACL6 does not exist, ACL-based packet filtering does not take effect.
ipv6	Specifies the IPv6 ACL configured for packet filtering.	- **NOTE** The S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S does not support IPv6 UCL.
name *acl-name*	Specifies the name of the user ACL or user ACL6 configured for packet filtering.	The value is a string of 1 to 64 case-sensitive characters without spaces and must begin with a letter. If the configured user ACL or user ACL6 does not exist, ACL-based packet filtering does not take effect.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In NAC network deployment, you can run the **ucl-group** command to classify users and configure user ACL or user ACL6 rules numbered from 6000 to 9999. You can then implement intra-group isolation (users in a group cannot communicate with each other) and inter-group isolation (users in the user group cannot communicate with users in other user groups.), and control network access rights based on the UCL group.

After configuring ACL rules 6000 to 9999, you must run the **traffic-filter acl** command to configure ACL-based packet filtering. The ACL rules then can take effect for the users in the UCL group.

Precautions

If you want to configure packet filtering through an authorized UCL group, run the **traffic-filter** command in a traffic profile to configure packet filtering and bind the traffic profile to a VAP profile. This ensures that packet filtering takes effect for the wireless users that go online on the same AP in the same VLAN.

If the user ACL specified in the **traffic-filter inbound acl** command or the user ACL or user ACL6 delivered by the authentication server is incorrectly configured to block all user traffic, the switch cannot be connected and network-side protocols such as OSPF and BGP are interrupted.

For a stack of S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, and S5720-LI: If the value of **RunningTemplate** is not **nac** in the **display system resource-template** command output on a member switch that forwards traffic out, user ACL6-based packet filtering configured using the **traffic-filter inbound acl ipv6** { *acl-number* | **name** *acl-name* } command in the system view does not take effect on the member switch.

Example

Configure the device to filter the packets in the inbound direction of the interface based on ACL 6001.

```
<HUAWEI> system-view
[HUAWEI] traffic-filter inbound acl 6001
```

13.5.248 traffic-redirect acl

Function

The **traffic-redirect acl** command configures ACL-based packet redirection.

The **undo traffic-redirect acl** command disables ACL-based packet redirection.

By default, ACL-based packet redirection is not configured.

NOTE

This command is supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI.

Format

traffic-redirect inbound acl { *acl-number* | **name** *acl-name* } [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *nexthop-address*

traffic-redirect inbound acl { *acl-number* | **name** *acl-name* } **vpn-instance** *vpn-instance-name*

undo traffic-redirect inbound acl { *acl-number* | **name** *acl-name* }

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **traffic-redirect inbound acl** { *acl-number* | **name** *acl-name* } **vpn-instance** *vpn-instance-name* command.

Parameters

Parameter	Description	Value
inbound	Configures packet redirection in the inbound direction of the interface.	-
acl *acl-number*	Specifies the ID of the ACL configured for packet redirection.	The value is an integer in the range from 6000 to 9999. If the configured user ACL does not exist, ACL-based packet redirection does not take effect.
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces and must begin with a letter. If the configured user ACL does not exist, ACL-based packet redirection does not take effect.
vpn-instance *vpn-instance-name*	Redirects packets to a VPN instance.	The value must be the name of an existing VPN instance.
ip-nexthop *nexthop-address*	Redirects packets to a next-hop IPv4 address.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In NAC network deployment, you can run the **ucl-group** command to classify users and configure user ACLs with numbers in the range of 6000 to 9999. You can then implement intra-group isolation (users in a group cannot communicate with each other) and inter-group isolation (users in the user group cannot communicate with users in other user groups), and control network access rights based on the UCL group.

After configuring ACLs with numbers in the range of 6000 to 9999, you can run the **traffic-redirect acl** command to configure ACL-based packet redirection. The ACLs then can take effect for the users in the UCL group.

When the **traffic-redirect** command and the **traffic-filter acl** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is redirected.

Precautions

If the destination address information about the packets to be filtered based on a user ACL rule contains UCL group, the ACL rule takes effect only for S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

If the destination address information about the packets to be filtered based on a user ACL rule contains UCL group, the ACL rule does not take effect.

Example

Configure the device to redirect the packets in the inbound direction of the interface based on ACL 6001.

```
<HUAWEI> system-view
[HUAWEI] traffic-redirect inbound acl 6001 ip-nexthop 192.168.1.1
```

13.5.249 ucl-group (service scheme view)

Function

The **ucl-group** command binds a UCL group to a service scheme.

The **undo ucl-group** command unbinds the UCL group from the service scheme.

By default, no UCL group is bound to a service scheme.

Format

ucl-group { *group-index* | **name** *group-name* }

undo ucl-group

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The UCL group must exist.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme** command, you can run the **ucl-group** command to bind a UCL group to the service scheme. The user assigned with the service scheme will have the functions of the UCL group.

Prerequisites

A UCL group has been created using the **ucl-group** command.

Example

Bind the UCL group **abc** to the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 10 name abc
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] ucl-group name abc
```

13.5.250 ucl-group domain

Function

The **ucl-group domain** command configures a domain name in a static UCL group.

The **undo ucl-group domain** command deletes a domain name from a static UCL group.

By default, no domain name is configured in a static UCL group.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support domain names in static UCL groups.

Format

ucl-group domain domain-name *domain-name* { *group-index* | **name** *group-name* }

undo ucl-group domain { **domain-name** *domain-name* | *group-index* | **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
domain-name *domain-name*	Specifies a domain name in a static UCL group.	The value is a string of 3 to 255 case-sensitive characters that can contain letters, digits, and special characters (_ . - *), but not spaces. A maximum of one asterisk (*) is supported. If a domain name contains an asterisk (*) at the beginning, the second character must be a period (.). If a domain name contains an asterisk (*) at the end, the last second character must be a period (.).
group-index	Specifies the index of a static UCL group.	The value is an integer in the range from 1 to 64000 for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 1 to 48 for the S6720-EI, S6720S-EI.
name *group-name*	Specifies the name of a static UCL group.	The value must be an existing UCL group name on the device.
all	Specifies all static UCL groups.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an enterprise network, a server that provides resources has a fixed domain name. The administrator can identify this server using a UCL group and associate the server domain name with the UCL group to form a static UCL group.

After a domain name of a resource server is configured in a static UCL group, the server IP addresses can be obtained based on this domain name and the user access policies can be managed based on the static UCL group, simplifying network deployment.

Prerequisites

A UCL group has been created using the **ucl-group** command.

Follow-up Procedure

Run the **dns snooping enable** command to enable DNS snooping.

Precautions

In the ubiquitous service solution, this command does not need to be run on the device, and it is configured on the controller and delivered to the device.

If the IP address obtained based on a domain name conflicts with the IP address configured using the **ucl-group ip** command, the configured IP address takes effect.

Currently, only IPv4 addresses can be obtained based on domain names.

In policy association and SVF scenarios, access devices do not support this command.

UCL groups do not support IP address overlapping. The device cannot allocate users or resources with the same IP addresses in different VPNs to different UCL groups, and can only allocate these users or resources to the same UCL group.

Example

Set the domain name in the static UCL group **email** to **example.com**.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 1 name email
[HUAWEI] ucl-group domain domain-name example.com name email
```

13.5.251 ucl-group ip

Function

The **ucl-group ip** command configures an IP address in a static UCL group. The static UCL group is also called the static resource group.

The **undo ucl-group ip** command deletes an IP address from a static UCL group.

By default, no IP address is configured in a static UCL group.

NOTE

IP addresses in static UCL groups are only supported by S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI.

Format

ucl-group ip *ip-address* { *mask-length* | *ip-mask* } { *group-index* | **name** *group-name* } [**escape**]

undo ucl-group ip { *ip-address* { *mask-length* | *ip-mask* } | *group-index* | **name** *group-name* | **all** }

undo ucl-group ip { *ip-address* { *mask-length* | *ip-mask* } | *group-index* | **name** *group-name* } **escape**

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a static UCL group. **NOTE** You can specify the IP address configured for the local device.	The value is in dotted decimal notation in the format X.X.X.X.
mask-length	Specifies the mask length of an IP address.	The value is an integer that ranges from 1 to 32.
ip-mask	Specifies the mask of the IP address.	The value is in dotted decimal notation.
group-index	Specifies the index of a static UCL group.	The value is an integer in the range from 1 to 64000 for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 1 to 48 for the S6720-EI, S6720S-EI.
name *group-name*	Specifies the name of a static UCL group.	The value must be an existing UCL group name on the device.
escape	Specifies an escape static UCL group.	-
all	Specifies all static UCL groups.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an enterprise network, a server that provides resources has a fixed IP address. The administrator can identify this server using a UCL group and associate the server IP address with the UCL group to form a static UCL group.

After a static UCL group is created for a resource server, the user access policies can be managed based on the static UCL group to simplify network deployment.

Prerequisites

A UCL group has been created using the **ucl-group** command.

Precautions

In the ubiquitous service solution, this command does not need to be run on the device, and it is configured on the controller and delivered to the device.

UCL groups do not support IP address overlapping. The device cannot allocate users or resources with the same IP addresses in different VPNs to different UCL groups, and can only allocate these users or resources to the same UCL group.

Example

Configure the static UCL group named **email** with the IP address 10.1.1.1/24.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 1 name email
[HUAWEI] ucl-group ip 10.1.1.1 24 name email
```

13.5.252 ucl-group (system view)

Function

The **ucl-group** command creates a UCL group.

The **undo ucl-group** command deletes the configured UCL group.

By default, no UCL group is created.

Format

ucl-group *group-index* [**name** *group-name*]

undo ucl-group { **all** | *group-index* | **name** *group-name* }

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The value is an integer in the range from 1 to 30 on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S. The value is an integer in the range from 1 to 48 on the S6720-EI, S6735-S, S6720S-EI. The value is an integer in the range from 1 to 64000 on the S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S5731-H, S5731S-H, S5731-S, S5731S-S.

Parameter	Description	Value
name *group-name*	Specifies the name of a UCL group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value cannot be -, --, a, an, or any, and cannot contain the following special characters: / \ : * ? " < > | @ ' %
all	Specifies the all UCL group.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In NAC network deployment, there are a large number of users and each user may be configured with many ACL rules. The ACL resources on the device are limited and therefore are insufficient to meet the demand of each user. If ACL rules are independently deployed for each user, the workload is heavy.

In actual NAC application, there are a large number of access users but the user types (users of a type have the same network access rights) are limited. The users can be classified using UCL groups (identify user types), and a group of ACL rules are deployed for users of the same type.

After you create UCL groups on the device and configure a UCL group for a user on the authentication server, the authentication server delivers the user's UCL group to the device when authenticating the user. In this way, the device obtains the mapping between users and UCL groups, and accordingly adds users to different UCL groups so that the users in each group can share the same ACL rules.

Follow-up Procedure

A UCL group only identifies a user type and does not control users' network access rights. To control the network access rights, you must first configure ACL rules numbered from 6000 to 9999 and then configure ACL-based packet filtering.

1. Run the **acl** command to create an ACL with the number range of 6000 to 9999.
2. Run the **rule (user ACL view)** to create rules for the ACL.
3. Run the **traffic-filter acl** command to configure ACL-based packet filtering.

Precautions

A UCL group cannot be deleted after it is referenced using any command for the S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI . For other models, a UCL group cannot be deleted after it is referenced using any command except **rule (user ACL view)**.

The UCL group and iStack functions are mutually exclusive for the S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI . A UCL group can be configured on the device only when it is deployed in a single-node system, the stack ID is 0, no stack port is configured, and no dedicated stack cable is installed. If a UCL group has been configured on the device, the stack ID cannot be changed, no stack port can be configured, and a stack cannot be automatically set up even if a dedicated stack cable is installed.

For the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S:

- In L3VPN scenarios, both static and dynamic UCL groups can be used to control packets sent from PEs to CEs, but only static UCL groups can be used to control packets sent from CEs to PEs.
- When IP packets are forwarded through MPLS LDP tunnels or MPLS TE tunnels, both static and dynamic UCL groups can be used to control the packets leaving the tunnels.
- In L2VPN scenarios, UCL groups cannot be used to control packets.

In the eMDI scenario, after the UCL group is successfully authorized for wireless users, modifying the UCL group configuration does not affect authorized users.

Example

Create a UCL group named **abc** with the group ID 10.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 10 name abc
```

13.5.253 user-queue single-user-mode

Function

The **user-queue single-user-mode** command sets the user queue scheduling mode to single-user mode.

The **undo user-queue single-user-mode** command restores the default configuration.

By default, user queue scheduling uses the user sharing mode.

NOTE

Only the S5731-S, S5731S-S, S5731-H, and S5731S-H switches support this command.

Format

user-queue single-user-mode

undo user-queue single-user-mode

Parameters

None

Views

System view, AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When HQoS is used to implement fine-granularity scheduling for authenticated users, the same user queue is used for scheduling traffic of users who use the same account for login by default. To implement fine-granularity scheduling for each user, run the **user-queue single-user-mode** command to set the user queue scheduling mode to single-user mode.

Follow-up Procedure

Run the **user-queue** command to create a user queue in the QoS profile to implement HQoS scheduling. The RADIUS server then delivers the QoS profile for new online users.

Precautions

- This command is not supported for wireless users.
- If you run this command in the system view, the configuration takes effect for all new users who go online on this device. If you run this command in an AAA domain, the configuration takes effect only for the new users in the AAA domain.
- When HQoS-based authorization is configured for wireless users, only the single-user mode is supported for user queue scheduling.

Example

Set the user queue scheduling mode to single-user mode in the system view.

```
<HUAWEI> system-view
[HUAWEI] user-queue single-user-mode
```

Set the user queue scheduling mode to single-user mode in the AAA domain view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] user-queue single-user-mode
```


13.5.254 url (URL template view)

Function

The **url** command configures a redirect URL or pushed URL.

The **undo url** command cancels a redirect URL or pushed URL.

By default, no redirect URL or pushed URL is configured.

Format

url [**push-only** | **redirect-only**] *url-string* [**ssid** *ssid*]

undo url [**push-only** | **redirect-only**] [**ssid** *ssid*]

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **ssid** *ssid* parameter.

Parameters

Parameter	Description	Value
url-string	Specifies a redirect URL or pushed URL.	The value is a string of 1 to 247 case-sensitive characters, with spaces and question marks (?) not supported. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
push-only	Specifies the URL only as a pushed URL.	-
redirect-only	Specifies the URL only as a redirect URL.	-
ssid *ssid*	Specifies the SSID that users associate with. This parameter is valid only for wireless access users. The SSID that users associate with must be the same as that configured on the device; otherwise, the device cannot push URLs to users.	The SSID must already exist.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a URL template is created using the **url-template name** command, you can run this command to configure a redirect URL or pushed URL. The difference between a redirect URL and a pushed URL is as follows:

- Redirect URL: When a user without network access permission attempts to access the network, the Portal authentication device redirects the user to the redirect URL for authentication.
- Pushed URL: After an authenticated user accesses the network through web for the first time, the access device pushes the web page corresponding to the URL to the user. The web access request from the user is redirected to the specified URL, and then the user is allowed to access network resources.

When you configure a URL on the device, question marks (?) are not supported. If a URL contains a question mark (?), you can run the **parameter start-mark #** command in the URL template view to replace the question mark (?) with a number sign (#).

Precautions

If the **push-only** and **redirect-only** parameters are not specified, the configured URL is used as both a redirect URL and a pushed URL. You can configure a pushed URL using the **force-push** command, or use the **url-template** command to bind a URL template to the Portal server template to configure a redirect URL.

Example

Set the redirect URL to http://10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.1
```

13.5.255 url (Portal server template view)

Function

The **url** command configures a URL for a Portal server.

The **undo url** command restores the default configuration.

By default, no URL is configured for a Portal server.

Format

url *url-string*

undo url

Parameters

Parameter	Description	Value
url-string	Specifies a URL for a Portal server.	The value is a string of 1 to 247 case-sensitive characters, with spaces and question marks (?) not supported. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the IP address of a Portal server is configured using the **server-ip** command (in the Portal server template view), the Portal server URL (http://*server-ip*) is generated by default on the device. If the actual URL of the Portal server is inconsistent with the default one or the domain name of the Portal server needs to be used for network access, you can run the **url** command to modify the URL of the Portal server on the device.

Precautions

A Portal server has only one URL.

Example

Set the URL of a Portal server to http://www.example.com in the Portal server template named **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] url http://www.example.com
```

13.5.256 url-parameter mac-address format

Function

The **url-parameter mac-address format** command configures the MAC address format in URL.

The **undo url-parameter mac-address format** command restores the default MAC address format in URL.

By default, the MAC address format in URL is XXXXXXXXXXXX.

Format

url-parameter mac-address format delimiter *delimiter* { **normal** | **compact** }

undo url-parameter mac-address format

Parameters

Parameter	Description	Value
delimiter *delimiter*	Specifies the delimiter in MAC address.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
normal	Sets the MAC address format to XX-XX-XX-XX-XX-XX.	-
compact	Sets the MAC address format to XXXX-XXXX-XXXX.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Portal servers or websites may require different MAC address formats. You can run the **url-parameter mac-address format** command to set MAC address formats in URL to meet the requirements of Portal servers or website.

Example

Set the delimiter to - and format to XXXX-XXXX-XXXX.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter mac-address format delimiter - compact
```

13.5.257 url-parameter

Function

The **url-parameter** command sets parameters in a URL.

The **undo url-parameter** command deletes parameters in a URL.

By default, a URL does not carry any parameters.

Format

url-parameter { **device-ip** *device-ip-value* | **device-mac** *device-mac-value* | **ap-ip** *ap-ip-value* | **ap-mac** *ap-mac-value* | **ssid** *ssid-value* | **login-url** *url-key url* | **redirect-url** *redirect-url-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* | **user-vlan** *user-vlan-value* | **ap-group-name** *ap-group-name-value* | **ap-location** *ap-location-value* | **ap-name** *ap-name-value* } *

undo url-parameter

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the following parameters: **ap-ip** *ap-ip-value*, **ap-mac** *ap-mac-value*, **ssid** *ssid-value*, **user-vlan** *user-vlan-value*, **ap-group-name** *ap-group-name-value*, **ap-location** *ap-location-value*, and **ap-name** *ap-name-value*.

Parameters

Parameter	Description	Value
device-ip *device-ip-value*	Specifies the IP address of the device carried in the URL and sets the parameter name displayed in the URL. In the wireless access scenario, the value of **device-ip** carried in the URL is the CAPWAP gateway address. In wired scenarios, the device cannot automatically obtain the device IP address, you can run the **url-parameter set device-ip** *ip-address* to specify the IP address.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
device-mac *device-mac-value*	Specifies the MAC address of the device carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Parameter	Description	Value
ap-ip *ap-ip-value*	Specifies the AP IP address carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users. **NOTE** When this parameter is specified in the AC + Fit central AP + RU scenario, the URL carries the name of the Fit central AP.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ap-mac *ap-mac-value*	Specifies the AP MAC address carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users. **NOTE** When this parameter is specified in the AC + Fit central AP + RU scenario, the URL carries the name of the Fit central AP.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ssid *ssid-value*	Specifies the users' associated SSID carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users.	The value is a string of 1 to 16 case-sensitive characters without spaces. Supported Chinese characters.If the string is enclosed in double quotation marks (" "), the string can contain spaces.
login-url *url-key url*	Specifies the login URL of an access device. • *url-key*: specifies the identification keyword for the login URL sent to the Portal server during redirection. • *url*: is a specified URL on the access device.	• *url-key*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *url*: The value is a string of 1 to 247 case-sensitive characters without spaces or Chinese characters.

Parameter	Description	Value
redirect-url *redirect-url-value*	Specifies the original URL that a user accesses carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
sysname *sysname-value*	Specifies the device system name carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
user-ipaddress *user-ipaddress-value*	Specifies the user IP address carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
user-mac *user-mac-value*	Specifies the user MAC address carried in the URL and sets the parameter name displayed in the URL. **NOTE** This parameter is recommended for inter-AC roaming scenarios.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. Cannot contain question marks. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Parameter	Description	Value
user-vlan *user-vlan-value*	Specifies the user VLAN carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wired users.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ap-group-name *ap-group-name-value*	Specifies the AP group name carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users.	The value is a string of 1 to 16 case-sensitive characters, without spaces or Chinese characters, and the following special characters not supported: =, ?, &.
ap-location *ap-location-value*	Specifies the AP location carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users. This parameter takes effect only for fit APs. Before setting this parameter, run the **location** command to configure the installation position of the AP.	The value is a string of 1 to 16 case-sensitive characters, without spaces or Chinese characters, and the following special characters not supported: =, ?, &.
ap-name *ap-name-value*	Specifies the AP name carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users. **NOTE** When this parameter is specified in the AC + Fit central AP + RU scenario, the URL carries the name of the Fit central AP.	The value is a string of 1 to 16 case-sensitive characters, without spaces or Chinese characters, and the following special characters not supported: =, ?, &.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a URL template is created using the **url-template name** command and URL is configured using the **url** command, you can use the **url-parameter** command to set the parameters in the URL. When a user accesses the Portal server according to the URL, the Portal server obtains user terminal information through the parameters in the URL. The Portal server then provides the corresponding web authentication page for the user according to user terminal information.

In addition, when users are redirected to a website rather than the Portal server according to the pushed URL, the website provides different web pages for the users according to user terminal information carried in the URL.

Precautions

In the wired access scenario, the **device-ip** parameter must be carried in a URL. In addition, you need to run the **url-parameter set device-ip** *ip-address* command to configure the value of **device-ip**, which is typically set to a WAN interface address.

In the policy association scenario, ASs do not support the **device-mac** and **sysname** parameters.

In policy association and SVF scenarios, the device does not support the **user-vlan** parameter.

URL parameter names configured on the device must be the same as those supported by the server. In this example, the device is connected to Agile Controller-Campus or iMaster NCE-Campus.

URL Parameter	URL Parameter Name Supported by Agile Controller-Campus / iMaster NCE-Campus
device-ip	ac-ip
ap-mac	apmac/ap-mac
ssid	ssid
redirect-url	url/redirect-url
user-ipaddress	userip/uaddress
user-mac	usermac/umac
user-vlan	uservlan

Example

Set the user MAC address and access device's system name in the URL.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter user-mac umac sysname test
```


13.5.258 url-parameter set

Function

The **url-parameter set** command sets redirection parameter values.

The **undo url-parameter set** command restores the default setting.

By default, the device automatically obtains redirection parameter values.

Format

url-parameter set device-ip *ip-address*

undo url-parameter set device-ip

Parameters

Parameter	Description	Value
device-ip *ip-address*	Sets the value of the redirection parameter **device-ip**.	The value is in dotted decimal notation.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Assume that a URL template is created using the **url-template name** command, and a URL is configured in the URL template using the **url** command. In the wireless access scenario, the default value of **device-ip** is the CAPWAP gateway address when STAs communicate with the Portal server. In the wired access scenario, the value of **device-ip** cannot be automatically obtained. In the wireless access scenario where communication using the default value fails or in the wired access scenario, run the **url-parameter set device-ip** *ip-address* command to set the redirection parameter (to the WAN interface address typically). When user terminals use the URL to access the Portal server, the Portal server then can obtain user terminal information according to parameters in the URL.

Example

Set the value of the redirection parameter **device-ip** to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter set device-ip 10.1.1.1
```


13.5.259 url-template name

Function

The **url-template name** command creates a URL template or displays an existing URL template view.

The **undo url-template name** command deletes a URL template.

By default, no URL template exists on the device.

Format

url-template name *template-name*

undo url-template name *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of a URL template.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a Portal authentication server template is created using the **web-auth-server** command, you can bind a URL template to the Portal authentication server template. The URL template contains the redirect URL and redirect URL parameters.

The **url-template name** command creates a URL template or displays an existing URL template view.

Example

Create a URL template named **test** and enter the template view.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
```


13.5.260 url-template (Portal server template view)

Function

The **url-template** command binds a URL template to a Portal server template.

The **undo url-template** command unbinds a URL template from a Portal server template.

By default, no URL template is bound to a Portal server template.

Format

url-template *url-template* [**ciphered-parameter-name** *ciphered-parameter-name* **iv-parameter-name** *iv-parameter-name* **key cipher** *key-string*]

undo url-template

Parameters

Parameter	Description	Value
url-template	Specifies the name of a URL template.	The value must be an existing URL template name.
ciphered-parameter-name *ciphered-parameter-name*	Specifies the name of the encrypted URL template parameter.	The value is a string of 1 to 16.
iv-parameter-name *iv-parameter-name*	Specifies the encryption vector name of the URL template parameter.	The value is a string of 1 to 16.
key cipher *key-string*	Specifies the shared key for encrypting the URL template parameter.	The value is a string of 1 to 16 plain-text characters or 48 cipher-text characters.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the parameters of a URL template are configured, the URL template must be bound to a Portal authentication server template so that users can be authenticated on the Portal authentication server corresponding to the redirect URL.

To ensure security, you can encrypt the parameter information in the URL template bound to the Portal server template.

Prerequisites

A URL template has been created using the **url-template name** command.

Precautions

If a URL template is bound to the Portal authentication server template and the **url** command is executed to configure the redirect URL corresponding to the Portal authentication server, only the parameters in the URL template take effect.

The URL configured using the **url** command in the URL template view cannot be a pushed URL; otherwise, the command does not take effect.

The device support encryption of parameter information in the URL template only when it connects to the Agile Controller-Campus or iMaster NCE-Campus.

Example

Bind the URL template **abc** to the Portal authentication server template.

```
<HUAWEI> system-view
[HUAWEI] url-template name abc
[HUAWEI-url-template-abc] quit
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] url-template abc
```

13.5.261 user-sync

Function

The **user-sync** command enables Portal authentication user information synchronization.

The **undo user-sync** command disables Portal authentication user information synchronization.

By default, Portal authentication user information synchronization is disabled.

Format

user-sync [**interval** *interval-period* | **max-times** *times*] *

undo user-sync

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the user information synchronization interval.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 300.
max-times *times*	Specifies the maximum number of user information synchronization failures.	The value is an integer that ranges from 2 to 255. The default value is 3.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If communication is interrupted because the network between the device and Portal server is disconnected or the Portal server is faulty, online Portal authentication users cannot go offline. Therefore, user information on the device and on the Portal server may be inconsistent and accounting may be inaccurate.

The **user-sync** command enables user information synchronization so that user information on the device and Portal server is synchronized at intervals to ensure user information consistency.

During information synchronization, the device does not disconnect the user immediately after detecting that the device has certain user information while the server does not have such information. Instead, the device disconnects the user when the maximum number of user information synchronization failures is reached.

Precautions

If users go online during the keepalive interval of the Portal server, the Portal server does not have their entries. After the Portal server goes Up and starts synchronizing user information, the device does not disconnect these users even if synchronization fails. The device retails these users until next time these users go online and performs Portal authentication, ensuring good user experience.

The value of *interval-period***times* configured on the device must be greater than the interval for the Portal server to send synchronization packets. Otherwise, the device may force users offline when it cannot receive any synchronization packet from the Portal server after the maximum failure number is reached.

When you run the **user-sync** command, make sure that the Portal server supports this function. Otherwise, the users will go offline.

Example

Enable user information synchronization in the Portal server template **abc**, set the interval for user information synchronization to 100s, and set the maximum number of synchronization failures to 5.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] user-sync interval 100 max-times 5
```

13.5.262 user-vlan (service scheme view)

Function

The **user-vlan** command configures a user VLAN in a service scheme.

The **undo user-vlan** command deletes the user VLAN configured in the service scheme.

By default, no user VLAN is configured in the service scheme.

Format

user-vlan *vlan-id*

undo user-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme** command, you can run the **vlan** command to configure a user VLAN in the service scheme. The user assigned with the service scheme will be added to the user VLAN and obtain network resources in the VLAN.

Precautions

An authorized VLAN cannot be delivered to online Portal users.

This command does not take effect for users who are already online.

If the user access mode is not **multi-share**, to make the **user-vlan** command take effect, you must configure the link type of access switches' interfaces connected to users to hybrid. Access switches will send untagged frames to users in the user VLAN even when interfaces connected users are added to this user VLAN in tagged mode.

For the S6735-S, S6720-EI, S6720S-EI When a user goes online through an interface and is authorized to a VLAN, the interface cannot access a BD in untagged mode. Otherwise, traffic cannot be forwarded.

Example

Configure user VLAN 100 in the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] user-vlan 100
```

13.5.263 voice-vlan (service scheme view)

Function

The **voice-vlan** command enables the voice VLAN in a service scheme.

The **undo voice-vlan** command restores the default setting.

By default, the voice VLAN is disabled in the service scheme.

Format

voice-vlan

undo voice-vlan

Parameters

None

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme** command, you can run the **voice-vlan** command to enable the voice VLAN in the service scheme. The voice user assigned with the service scheme will be added to the voice VLAN and obtain network resources in the VLAN.

Precautions

- An authorized VLAN cannot be delivered to online Portal users.
- To make this command take effect, you must have run the **voice-vlan enable** command to configure a specified VLAN as the voice VLAN and enable the voice VLAN on the interface.
- If the user access mode is set to **multi-share**, authorized voice VLANs are not supported.
- This command takes effect only to authorization of users who fail to be authenticated (configured using the **authentication event authen-fail action authorize** or **authentication event authen-server-down action authorize** command, and the **voice-vlan mac-address** command must be run to configure the OUI of the voice VLAN) or voice terminals who can go online without authentication (configured using the **authentication device-type voice authorize** command).
- This command takes effect only for the following users:
  - Users for whom the **authentication event authen-fail action authorize** or **authentication event authen-server-down action authorize** command is run to configure authorization in case of authorization failures or authentication server Down events and the **voice-vlan mac-address** command is run to configure the OUI address of the voice VLAN
  - Users for whom the **authentication device-type voice authorize** command is run to enable voice terminals to go online without authentication
- The following authorized VLANs are listed in descending order of their priorities: voice VLAN configured using the **lldp tlv-enable med-tlv network-policy voice-vlan** command > voice VLAN authorized by the server > voice VLAN authorized locally > data VLAN authorized by the server > data VLAN authorized locally.

Example

Enable the voice VLAN in the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] voice-vlan
```

13.5.264 vpn-instance (Portal server template view)

Function

The **vpn-instance** command configures a VPN instance used for communication between the device and Portal server.

The **undo vpn-instance** command restores the default setting.

By default, no VPN instance is configured for communication between the device and Portal server.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VPN implements interconnection within the same department and between different departments in an enterprise. To enable the Portal authentication service in the VPN, run the **vpn-instance** command to bind a Portal server template to a VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

The VPN instance bound to the Portal server template must be the same as that bound to the Portal server.

The users in VPN instances bound to different Portal server templates cannot use the same IP addresses because users with the same IP addresses cannot go online or offline.

Example

Bind the Portal server template **abc** to the VPN instance **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
```



```
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] vpn-instance vpn1
```

13.5.265 web-auth-server listening-port

Function

The **web-auth-server listening-port** command sets the number of the port through which a device listens on Portal protocol packets.

The **undo web-auth-server listening-port** command restores the default listening port.

By default, the device uses port 2000 to listen on Portal protocol packets.

Format

web-auth-server listening-port *port-number*

undo web-auth-server listening-port

Parameters

Parameter	Description	Value
port-number	Specifies the number of the listening port.	The value is an integer that ranges from 1024 to 55535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device exchanges user authentication information with the Portal server using the Portal protocol, you must configure the listening port on the device to receive Portal packets.

You can run the **web-auth-server listening-port** command to set the number of the port through which the device listens on Portal packets. The port number must be the same as the destination port number in Portal packets sent by the Portal server and must be unique.

NOTE

If a specified port is occupied by another service or is a reserved port, the configuration fails. Ensure that the specified port is available when running this command.

Example

Set the number of the port through which a device listens on Portal protocol packets to 3000.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server listening-port 3000
```

13.5.266 web-auth-server (Portal access profile view)

Function

The **web-auth-server** command configures the Portal server template used by a Portal access profile.

The **undo web-auth-server** command restores the default setting.

By default, a Portal access profile does not use any Portal server template.

Format

web-auth-server *server-name* [*bak-server-name*] { **direct** | **layer3** }

undo web-auth-server

Parameters

Parameter	Description	Value
server-name	Specifies the name of a Portal server template.	The value must be an existing Portal server template name.
bak-server-name	Specifies the name of a backup Portal server template. **NOTE** The name of the backup Portal server template cannot be configured to the command-line keywords **direct** and **layer3**.	The value must be an existing Portal server template name.
direct	Sets the Portal authentication mode to Layer 2 authentication.	-
layer3	Sets the Portal authentication mode to Layer 3 authentication.	-

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Portal server template is configured on the device, this profile must be bound to a Portal access profile. When users who use the Portal access profile attempt to access charged network resources, the HTTP requests are forcibly redirected to the authentication page of the Portal server to implement Portal authentication.

To improve Portal authentication reliability, the backup Portal server template can also be bound to the Portal access profile. When the primary Portal server is disconnected, the users are redirected to the backup Portal server for authentication. This function can take effect only when the Portal server detection function is enabled using the **server-detect** command and heartbeat detection is enabled on the Portal server.

The following Portal authentication modes are available:

- **direct**: When there is no Layer 3 forwarding device between the device and a user, the device can learn the user's MAC address. You can configure the Layer 2 authentication mode so that the device can identify the user using the MAC address.
- **layer3**: Whether Layer 3 forwarding devices exist between the user and device, the MAC address table of the device cannot learn the user's MAC address and can only identify the user using the IP address. You need to configure the Layer 3 authentication mode.

Prerequisites

A Portal server template has been created using **web-auth-server** and the IP address of the Portal server has been configured using **server-ip**.

Precautions

- After a Portal access profile is bound to an authentication profile, the Portal server template used in the Portal access profile cannot be deleted, but can be modified.
- The support for Portal authentication varies depending on different interfaces, routed main interfaces (Only S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI) support only Layer 3 Portal authentication, Layer 2 interfaces support only Layer 2 Portal authentication, and VLANIF interfaces support both Layer 2 and Layer 3 Portal authentication.
- This command does not take effect on the VLANIF interface corresponding to the super VLAN.
- When the direct forwarding mode is used for wireless users and Portal authentication is enabled on the VLANIF interface, the branched networking must be used for the device to make Portal authentication take effect.

Example

Bind the Portal access profile **p1** to the Portal server templates **server1** and **server2** (backup Portal server template), and configure the Layer 2 authentication mode.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server server1
[HUAWEI-web-auth-server-server1] server-ip 10.10.1.1
[HUAWEI-web-auth-server-server1] quit
[HUAWEI] web-auth-server server2
[HUAWEI-web-auth-server-server2] server-ip 10.10.2.1
[HUAWEI-web-auth-server-server2] quit
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] web-auth-server server1 server2 direct
```

13.5.267 web-auth-server reply-message

Function

The **web-auth-server reply-message** command enables the device to transparently transmit users' authentication responses sent by the authentication server to the Portal server.

The **undo web-auth-server reply-message** command disables the device from transparently transmitting users' authentication responses sent by the authentication server to the Portal server.

By default, the device transparently transmits users' authentication responses sent by the authentication server to the Portal server.

Format

web-auth-server reply-message

undo web-auth-server reply-message

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The AAA server requires that the authentication messages sent to the Portal server contain the authentication reply; therefore, the **web-auth-server reply-message** command is required. In certain situations, the authentication messages are not required to carry the reply. In this case, run the **undo web-auth-server reply-message** command.

By default, the device directly forwards the authentication result message from the RADIUS server to the Portal server without processing. This is called transparent transmission.

Example

Disable the device from transparently transmitting users' authentication responses to the Portal server.

```
<HUAWEI> system-view
[HUAWEI] undo web-auth-server reply-message
```

13.5.268 web-auth-server (system view)

Function

The **web-auth-server** command creates a Portal server template or displays the Portal server template view.

The **undo web-auth-server** command deletes a Portal server template.

By default, no Portal server template exists.

Format

web-auth-server *server-name*

undo web-auth-server *server-name*

Parameters

Parameter	Description	Value
server-name	Specifies the name of a Portal server.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --. **NOTE** *server-name* cannot be set to listening-port, reply-message, version, server-source, or the first character or several leftmost characters of these character strings.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Portal user goes online, the device redirects the user to a specified website (also called the portal website). The user can access resources in the website for free. When the user attempts to access charged network resources, the user must pass authentication on the website. The specific process is as follows:

1. The user opens Internet Explorer and enters a URL in the address box. When receiving the HTTP request sent by the user, the device redirects it to the Portal authentication page of the Portal server.
2. The user enters user information on the authentication page or in the authentication dialog box, and the Portal server forwards the user information to the device.
3. After receiving the user information from the Portal server, the device sends the information to the authentication server for authentication and accounting.
4. After the user is authenticated, the device allows the user to access the Internet if no security policy is enforced.

After a Portal server template is created on the device by using the **web-auth-server** command, run other commands to create a route from the device to the Portal server.

Follow-up Procedure

Run the following commands in the Portal server template view to configure related attributes:

- Run the **server-ip** command to configure the IP address of a Portal server.
- Run the **url** command to configure the URL of a Portal server.
- Run the **port** command to set the port number that a Portal server uses to receive packets from the device.
- Run the **shared-key** command to configure the shared key that the device uses to exchange information with the Portal server.

Precautions

You are advised to back up the Portal server data to prevent authentication failure caused by the Portal server fault.

V200R020C10SPC100 and later versions: If Portal authentication is enabled on the device, you must configure the local gateway address used by the device to receive and respond to the packets sent by the Portal server. You can use either of the following methods to configure the address:

- Run the **web-auth-server server-source all-interface** command in the system view.
- Run the **server-source ip-address** *ip-address* command in the Portal server template view.

Example

Create Portal server template named **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
```

13.5.269 web-auth-server server-source (system view)

Function

The **web-auth-server server-source** command configures the local gateway address used by the device to receive and respond to the packets sent by the Portal server when Portal authentication is enabled.

The **undo web-auth-server server-source** command restores the default configuration.

By default, the device does not receive any packets from the Portal server.

Format

web-auth-server server-source all-interface

undo web-auth-server server-source all-interface

Parameters

Parameter	Description	Value
all-interface	Indicates that the IPv4 address is set to 0.0.0.0. That is, the device can receive and respond to all packets sent by the Portal server.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

V200R020C10SPC100 and later versions: If Portal authentication is enabled on the device, you must configure the local gateway address used by the device to receive and respond to the packets sent by the Portal server. You can use either of the following methods to configure the address:

- Run the **web-auth-server server-source all-interface** command in the system view.
- Run the **server-source ip-address** *ip-address* command in the Portal server template view.

Precautions

- If the system software of the device is upgraded from a version earlier than V200R020C10SPC100 to a later version and Portal authentication is enabled, the device delivers the **web-auth-server server-source all-interface** command by default.
- After the **web-auth-server server-source all-interface** command is run, the system clears all configurations of the **server-source ip-address** *ip-address* command.
- If the **web-auth-server server-source all-interface** command has been configured on the device, the **server-source ip-address** *ip-address* command configured later will fail to be delivered.

Example

In the system view, configure the device to receive and respond to all packets sent by the Portal server.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server server-source all-interface
```

13.5.270 web-auth-server version

Function

The **web-auth-server version** command sets the Portal protocol version supported by the device.

The **undo web-auth-server version** command restores the default setting.

By default, the device supports both the versions V1.0 and V2.0.

Format

web-auth-server version v2 [**v1**]

undo web-auth-server version

Parameters

Parameter	Description	Value
v2	Indicates that the device supports the Portal protocol version V2.0. The major version currently used is V2.0.	-
v1	Indicates that the device supports the Portal protocol version V1.0.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Currently, the Portal protocol has two versions: V1.0 and V2.0. The device and Portal server must use the Portal protocol of the same version to ensure normal communication. You can run the **web-auth-server version** command to set the Portal protocol version supported by the device.

NOTE

The version V2.0 is widely used currently.

To ensure smooth communication, the device supports both versions by default.

Example

Configure the device to use only the Portal protocol V2.0.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server version v2
```

13.5.271 web-redirection disable (Portal server template view)

Function

The **web-redirection disable** command disables the Portal authentication redirection function.

The **undo web-redirection disable** command enables the Portal authentication redirection function.

By default, the Portal authentication redirection function is enabled.

Format

web-redirection disable

undo web-redirection disable

Parameters

None

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

The device redirects all unauthenticated users to the Portal authentication page when the users send access requests to external networks. For example, when the user needs to enter the URL of the authentication page manually, the **web-redirection disable** command can be executed so that unauthorized users are not forcibly redirected to the Portal authentication page.

Example

Disable the Portal authentication redirection function.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server nac
[HUAWEI-web-auth-server-nac] web-redirection disable
```

13.6 NAC Configuration Commands (Common Mode)

13.6.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.6.2 access-user arp-detect

Function

The **access-user arp-detect** command sets the source IP address and source MAC address of offline detection packets in a VLAN.

The **undo access-user arp-detect** command deletes the source IP address and source MAC address of offline detection packets in a VLAN.

By default, the source IP address and source MAC address are not specified for offline detection packets in a VLAN.

Format

access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

undo access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
ip-address *ip-address*	Specifies the source IP address of offline detection packets.	The value is in dotted decimal notation and can be 0.0.0.0 or 255.255.255.255 or other valid IP address.
mac-address *mac-address*	Specifies the source MAC address of offline detection packets.	The value is a unicast MAC address in H-H-H format, where H can be one to four hexadecimal digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

If the VLAN to which the user belongs does not have a VLANIF interface or the VLANIF interface does not have an IP address, the device sends an offline detection packet using 0.0.0.0 as the source IP address. If a user cannot respond to an ARP probe packet with the source IP address 0.0.0.0, you can specify a source IP address for the offline detection packet. You are advised to specify the user gateway IP address and its corresponding MAC address as the source IP address and source MAC address of offline detection packets.

Precautions

This function does not take effect for users who use Layer 3 Portal authentication.

If a user on a physical interface is online, this command takes effect only after the user goes online again or the device re-authenticates the user.

Example

Set the source IP address and MAC address of offline detection packets for users in VLAN 10 to 192.168.1.1 and 2222-1111-1234 respectively.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect vlan 10 ip-address 192.168.1.1 mac-address 00e0-fc11-1234
```

13.6.3 access-user arp-detect default ip-address

Function

The **access-user arp-detect default ip-address** command sets the default source IP address of offline detection packets.

The **undo access-user arp-detect default ip-address** command restores the default setting.

By default, the default source IP address of offline detection packets is 0.0.0.0.

Format

access-user arp-detect default ip-address *ip-address*

undo access-user arp-detect default ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the default source IP address of offline detection packets.	The value is in dotted decimal notation and can be 0.0.0.0 or other valid IP address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

Precautions

This function does not take effect for users who use Layer 3 Portal authentication.

Example

Set the default source IP address of offline detection packets to 0.0.0.0.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect default ip-address 0.0.0.0
```

13.6.4 access-user arp-detect delay

Function

The **access-user arp-detect delay** command configures the delay in sending offline detection packets.

The **undo access-user arp-detect delay** command restores the default configuration.

By default, the delay in sending offline detection packets is 10 seconds.

Format

access-user arp-detect delay *delay*

undo access-user arp-detect delay

Parameters

Parameter	Description	Value
delay	Specifies the delay in sending offline detection packets.	The value is an integer in the range from 10 to 120, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A Windows client on the network sends a detection packet with the source address 0.0.0.0 after obtaining an IP address. If the device also initiates an ARP probe with the source address 0.0.0.0, a conflict occurs. To prevent this conflict, you can run the **access-user arp-detect delay** command to set the delay in sending offline detection packets. Typically, detection initiated by a Windows client takes 10 seconds. Therefore, a delay longer than 10 seconds is recommended.

Precautions

This function takes effect only for users who go online after it is configured.

This function takes effect in both ARP probe and ND probe scenarios.

NOTE

Delay after which the device sends the first ARP probe packet = Delay in sending offline detection packets + One-third of the handshake interval between the device and pre-connection or authorized users (configured using the **authentication timer handshake-period** command)

Example

Set the delay for sending offline detection packets to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect delay 20
```

13.6.5 access-user arp-detect fallback

Function

The **access-user arp-detect fallback** command configures an IP address required for calculating the source address of offline detection packets.

The **undo access-user arp-detect fallback** command deletes the IP address configured for calculating the source address of offline detection packets.

By default, no IP address is configured for the device to calculate the source address of offline detection packets.

Format

access-user arp-detect fallback *ip-address* { *mask* | *mask-length* }

undo access-user arp-detect fallback

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address required for calculating the source address of offline detection packets.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address.	The value is in dotted decimal notation. After the mask is converted into a binary number, all bits before the last 1 must be 1s. That is, 1s in the mask must be continuous and there cannot be any 0s before the last 1.

Parameter	Description	Value
mask-length	Specifies the mask length of the IP address.	The value is an integer in the range from 0 to 32.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device does not function as a gateway, it can send offline detection packets with the source address on the same network segment as clients. This source address is calculated based on the client network segment and the IP address specified in the **access-user arp-detect fallback** command. The operation AND is performed between this specified IP address and the wildcard mask to obtain result 1. Then result 1 is added to the network segment of clients to get the source address of offline detection packets. For example, if the network segment of clients is 192.168.1.0/24 and **access-user arp-detect fallback 0.0.0.11 24** is configured, the source address of offline detection packets is 192.168.1.11. The calculated source address must be excluded from the address pool of the DHCP server to prevent IP address conflicts.

Precautions

Only wired users support this function.

This function does not take effect for users who use Layer 3 Portal authentication.

For online users on physical interfaces, this command takes effect only after the users go online again or the device re-authenticates the users. For online users on Eth-Trunk interfaces, this command takes effect immediately.

- The source IP or MAC addresses configured for offline detection packets using the following commands are listed in descending order of priority:
  - **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*
  - **access-user arp-detect fallback** *ip-address* { *mask* | *mask-length* }
  - **access-user arp-detect default ip-address** *ip-address*

  If two or more of the commands are configured, the source IP or MAC address with a higher priority takes effect.

Example

Set the IP address required for calculating the source address of offline detection packets to 0.0.0.11.


```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect fallback 0.0.0.11 24
```

13.6.6 access-user dot1x-identity speed-limit

Function

The **access-user dot1x-identity speed-limit** command configures the rate limit of Identity packets for 802.1X authentication to be sent to the CPU.

The **undo access-user dot1x-identity speed-limit** command restores the default rate limit of Identity packets for 802.1X authentication to be sent to the CPU.

By default, the maximum of Identity packets for 802.1X authentication can be sent to the CPU every second depends on the device.

Format

access-user dot1x-identity speed-limit *value*

undo access-user dot1x-identity speed-limit [*value*]

Parameters

Parameter	Description	Value
value	Specifies the rate limit of Identity packets for 802.1X authentication to be sent to the CPU.	The value is an integer in the range of 5 to 2000, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a large number of Identity packets for 802.1X authentication are sent to the CPU of a switch, the CPU usage is high and other services are affected. To prevent this problem, run the **access-user dot1x-identity speed-limit** command to configure the rate limit of Identity packets for 802.1X authentication to be sent to the CPU, so that the switch discards excess Identity packets.

Example

Set the rate limit of Identity packets for 802.1X authentication to be sent to the CPU to 10 pps.


```
<HUAWEI> system-view
[HUAWEI] access-user dot1x-identity speed-limit 10
```

13.6.7 access-user syslog-restrain enable

Function

The **access-user syslog-restrain enable** command enables system log suppression.

The **undo access-user syslog-restrain enable** command disables system log suppression.

By default, system log suppression is enabled.

Format

access-user syslog-restrain enable

undo access-user syslog-restrain enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a user fails in authentication or goes offline, the device records a system log. The system log contains the MAC addresses of access device and access user and the authentication time.

If a user repeatedly attempts to go online after authentication failures or frequently goes online and offline in a short period, a lot of system logs are generated, which waste system resources and degrade system performance. System log suppression can address this problem. After the device generates a system log, it will not generate the same log within the suppression period (set by **access-user syslog-restrain period**).

NOTE

The same system logs refer to the system logs containing the same MAC addresses. For example, after the device generates a system log for a user failing in authentication, the device will not generate new system log for this user in the suppression period if the user fails in authentication again. The system logs for users logging offline are generated in the same way.

Example

Enable system log suppression.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain enable
```

13.6.8 access-user syslog-restrain period

Function

The **access-user syslog-restrain period** command sets a period for system log suppression.

The **undo access-user syslog-restrain period** command restores the default period for system log suppression.

By default, the period of system log suppression is 300s.

Format

access-user syslog-restrain period *period*

undo access-user syslog-restrain period

Parameters

Parameter	Description	Value
period	Specifies the period for system log suppression.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the system log suppression function is enabled using the **access-user syslog-restrain enable** command, use this command to set the system log suppression period. After generating a system log, the device will not generate the same log within the suppression period.

Example

Set the period for system log suppression to 600s.


```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain period 600
```

13.6.9 acl authorization statistics enable

Function

The **acl authorization statistics enable** command enables statistics collection on packets that match the ACLs assigned for authorization.

The **undo acl authorization statistics enable** command disables statistics collection on packets that match the ACLs assigned for authorization.

By default, statistics collection on packets that match the ACLs assigned for authorization is disabled.

Format

acl authorization statistics enable

undo acl authorization statistics enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a live network, the authentication server may assign ACLs to users who pass NAC authentication to grant the users access to the network. You can run the **acl authorization statistics enable** command to check the number of user packets that match the assigned ACLs.

Precautions

The function takes effect only for users who go online after this function is enabled, and for the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, and S5720-LI, this function cannot be used to collect statistics on packets that match the permit rules in redirection ACLs.

Example

Enable statistics collection on packets that match the ACLs assigned for authorization.


```
<HUAWEI> system-view
[HUAWEI] acl authorization statistics enable
```

13.6.10 acl-id (user group view)

Function

The **acl-id** command binds an ACL to a user group.

The **undo acl-id** command unbinds an ACL from a user group.

By default, no ACL is bound to a user group.

Format

acl-id *acl-number*

undo acl-id { *acl-number* | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL bound to a user group.	The value is an integer that ranges from 3000 to 3999.
all	Deletes all ACL rules bound to a user group.	-

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a user group is created using the **user-group** command, you can run the **acl-id** *acl-number* command to bind an ACL to the user group, so that users in the user group share an ACL.

NOTE

Before an ACL is bound to the user group, do not run the **user-group enable** command to enable the user group; otherwise, the ACL cannot be bound to the user group.

When the user group function is enabled on models except the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, ACL rules are delivered to each user and the user group function cannot be used to save ACL resources.

Prerequisites

The ACL has been created using the **acl** or **acl name** command and ACL rules have been configured using the **rule** command.

Precautions

- The ACL bound to a user group cannot be modified or deleted in the system view.
- If no ACL rule is configured for a user group, the device does not restrict the network access rights of users in the user group.
- When configuring ACL rules in a user group, create a rule that rejects all network access requests and ensure that the rule can take effect.
- If all users in a group are required to have the same access rights, do not specify the source IP address in the ACL bound to the user group. If an ACL bound to a user group has defined the source IP address, only users with the same IP address as the source IP address in the ACL can match the ACL in the user group.

Example

Bind ACL 3001 to the user group **abc**.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule 5 deny ip destination 192.168.5.0 0.0.0.255
[HUAWEI-acl-adv-3001] quit
[HUAWEI] user-group abc
[HUAWEI-user-group-abc] acl-id 3001
```

13.6.11 authentication critical eapol-success

Function

The **authentication critical eapol-success** command configures the device to send an EAPoL-Success packet to a user after the user is added to the critical VLAN.

The **undo authentication critical eapol-success** command configures the device to send an EAPoL-Fail packet to a user after the user is added to the critical VLAN.

By default, an EAPoL-Fail packet is sent to a user after the user is added to the critical VLAN.

Format

In the system view:

authentication critical eapol-success interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication critical eapol-success interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication critical eapol-success

undo authentication critical eapol-success

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After a user is added to the critical VLAN because the authentication server does not respond, the device can be configured to send an EAPoL-Success or EAPoL-Fail packet to the user to prevent the user from continuously sending access request packets. After receiving the EAPoL-Success packet or EAPoL-Fail packet, the user stops attempting to go online by sending the access request packet repeatedly, which prevents the device performance from degrading.

The user receiving the EAPoL-Success packet can still obtain the IP address through a DHCP packet, while the user receiving the EAPoL-Fail packet fails to do so. The administrator can configure the device to send an EAPoL-Success or EAPoL-Fail packet as required.

Example

Configure the device to send an EAPoL-Success packet to a user after the user is added to the critical VLAN on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication critical eapol-success
```


13.6.12 authentication critical-vlan

Function

The **authentication critical-vlan** command configures a critical VLAN on an interface.

The **undo authentication critical-vlan** command deletes a critical VLAN from an interface.

By default, no critical VLAN is configured on an interface.

Format

In the system view:

authentication critical-vlan *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication critical-vlan [*vlan-id*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication critical-vlan *vlan-id*

undo authentication critical-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of a critical VLAN.	The value is an integer that ranges from 1 to 4094.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A critical VLAN is authorized for users when the authentication server does not respond.

When the access device cannot communicate with the RADIUS server or the RADIUS server fails, the authentication process on the network is interrupted and users cannot pass the authentication. After the critical VLAN function of the device is enabled, the device sets the state flag of the authentication server to Down and adds the users to the critical VLAN. In this way, the users can access resources in the critical VLAN without being authenticated.

Precautions

- This command is only valid for 802.1X authentication and MAC address authentication.
- If the free-ip function is configured, the critical VLAN function becomes invalid immediately.
- To make the VLAN authorization function take effect, the link type and access control mode of the authentication interface must meet the following requirements:
  - When the link type is hybrid in untagged mode, the access control mode can be based on the MAC address or interface.
  - When the link type is access or trunk, the access control mode can only be based on the interface.

Example

In the system view, configure 802.1X authentication for the users using Port address-based access method on GE0/0/1 and set the critical VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] dot1x enable interface gigabitethernet 0/0/1
[HUAWEI] dot1x port-method port interface gigabitethernet 0/0/1
[HUAWEI] authentication critical-vlan 20 interface gigabitethernet 0/0/1
```

In the interface view, enable MAC address authentication on GE0/0/1 and set the critical VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] mac-authen
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] mac-authen
[HUAWEI-GigabitEthernet0/0/1] authentication critical-vlan 20
```


13.6.13 authentication device-type voice authorize

Function

The **authentication device-type voice authorize** command enables voice terminals to go online without authentication.

The **undo authentication device-type voice authorize** command disables voice terminals from going online without authentication.

By default, voice terminals are disabled from going online without authentication.

Format

authentication device-type voice authorize [**user-group** *group-name*]

undo authentication device-type voice authorize [**user-group**]

Parameters

Parameter	Description	Value
user-group *group-name*	Specifies the name of the user group based on which network access rights are assigned to voice terminals.	The value must be an existing user group name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both data terminals (such as PCs) and voice terminals (such as IP phones) are connected to switches, NAC is configured on the switches to manage and control the data terminals. The voice terminals, however, only need to connect to the network without being managed and controlled. In this case, you can configure the voice terminals to go online without authentication on the switches. Then the voice terminals identified by the switches can go online without authentication.

Precautions

To enable the switches to identify the voice terminals, enable LLDP or configure OUI for the voice VLAN on the switches. For details, see "Configuring Basic LLDP Functions" in "LLDP Configuration" in the *S300, S500, S2700, S5700, and S6700*

V200R023C00 Configuration Guide - Network Management and Monitoring or "Configuring a Voice VLAN Based on a MAC Address" in "Voice VLAN Configuration" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Ethernet Switching*. If a voice device supports only CDP but does not support LLDP, configure CDP-compatible LLDP on the switch using **lldp compliance cdp receive** command.

If an 802.1X user initiates authentication through a voice terminal, a switch preferentially processes the authentication request. If the authentication succeeds, the terminal obtains the corresponding network access rights. If the authentication fails, the switch identifies the terminal type and enables the terminal to go online without authentication.

Voice terminals can obtain the corresponding network access rights after they pass authentication and go online, when **user-group** *group-name* is not specified. When **user-group** *group-name* is specified, voice terminals can obtain the network access rights specified by the user group after they go online. To use a user group to define network access rights for voice terminals, run the **user-group** *group-name* command to create a user group and configure network authorization information for the users in the group. Note that the user group takes effect only after it is enabled.

If you run this command repeatedly, the latest configuration overrides the previous ones.

This function takes effect only for users who go online after this function is successfully configured.

Example

Enable voice terminals to go online without authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication device-type voice authorize
```

13.6.14 authentication event

Function

The **authentication event** command grants network access rights to users in different authentication stages.

The **undo authentication event** command cancels network access rights of users in different authentication stages.

By default, no network access right is granted to users in different authentication stages.

Format

- Command for 802.1X authentication:

  System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view:

  authentication event { **pre-authen** | **authen-fail** | **authen-server-down** | **client-no-response** } { **vlan** *vlan-id* | **user-group** *group-name* }

undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** | **client-no-response** }

- Command for MAC address authentication:

  System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view:

  authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } { **vlan** *vlan-id* | **user-group** *group-name* }

  undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** }

  VLANIF interface view:

  authentication event { **authen-fail** | **authen-server-down** } **user-group** *group-name*

  undo authentication event { **authen-fail** | **authen-server-down** }

- Command for external Portal authentication:

  System view:

  authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } **user-group** *group-name*

  undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** }

  VLANIF interface view:

  authentication event { **authen-fail** | **authen-server-down** } **user-group** *group-name*

  undo authentication event { **authen-fail** | **authen-server-down** }

- Command for built-in Portal authentication:

  System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view:

  authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } { **vlan** *vlan-id* | **user-group** *group-name* }

  undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** }

  VLANIF interface view:

  authentication event { **authen-fail** | **authen-server-down** } **user-group** *group-name*

  undo authentication event { **authen-fail** | **authen-server-down** }

Parameters

Parameter	Description	Value
pre-authen	Specifies the network access rights granted to users before authentication starts. In an 802.1X authentication, when a device receives an ARP or DHCP request packet sent from a user terminal, but not an authentication request packet from an 802.1X client, the device grants the **pre-authen** right to the user. If only this parameter is specified but the network access rights are not configured for other events, the device grants the **pre-authen** right to the users failing in authentication. In a MAC address or Portal authentication, if only this parameter is specified but the network access rights are not configured for other events, the device grants the **pre-authen** right to the users failing in authentication.	-
authen-fail	Specifies the network access rights granted to users when authentication fails. The device grants this right to all users who have failed in authentication.	-
authen-server-down	Specifies the network access rights granted to users when the authentication server does not respond. If both the **authen-server-down** and **authen-fail** parameters are specified, the **authen-server-down** parameter takes effect if the authentication server does not respond.	-
client-no-response	Specifies the network access rights granted to users when the 802.1X client does not respond. If both the **client-no-response** and **authen-fail** parameters are specified, the **client-no-response** parameter takes effect if the 802.1X client does not respond.	-

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID. When this parameter is specified, the user can access only the resources in the VLAN.	The value is an integer that ranges from 1 to 4094. The VLAN must exist on the device. Otherwise, the configuration does not take effect.
user-group *group-name*	Specifies a user group. When this parameter is specified, the user can access the resources defined for the user group.	The value must be an existing service scheme name.

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To grant different network access rights to users in different stages, you can use this command.

Prerequisites

The 802.1X authentication, MAC address authentication, or Portal authentication has been enabled.

Precautions

- If the command is executed in both the interface view and system view, the configuration in interface view takes effect.
- This function takes effect only for users who go online after this function is successfully configured.
- If the **user-group** parameter is specified in the command, only the network access rights (that is, the ACL and VLAN bound to the user group) configured for the user group take effect.
- If the network access rights specified in the **authentication event** command were defined by a user group, the **dot1x free-ip** command configured in the system view cannot take effect and the **dot1x free-ip** command configured in the interface view does not take effect for the interface.

- If the **user-group** parameter is specified in the command and the destination network access rights in the authentication-free rule configured by **portal free-rule** is the same as that defined for the user group, the authentication-free rule does not take effect.

Example

On GE0/0/1, allow users to access resources in VLAN 10 when authentication fails.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication event authen-fail vlan 10
```

13.6.15 authentication event response-fail

Function

The **authentication event response-fail** command configures the device to return an authentication failure packet when a user fails in authentication or the authentication server does not respond.

The **undo authentication event response-fail** command restores the default configuration.

By default, the device returns an authentication success packet when a user fails in authentication or the authentication server does not respond.

Format

authentication event { **authen-fail** | **authen-server-down** } **response-fail**

undo authentication event { **authen-fail** | **authen-server-down** } **response-fail**

Parameters

Parameter	Description	Value
authen-fail	Specifies that the device returns an authentication failure packet to the 802.1X client or Portal server when a user fails in authentication.	-
authen-server-down	Specifies that the device returns an authentication failure packet to the 802.1X client or Portal server when the authentication server does not respond.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **authentication event** command is executed to configure the network access right used when a user fails in authentication or the authentication server does not respond, the device returns an authentication success packet to the 802.1X client or Portal server by default. Therefore, the user does not know the authentication failure and only limited network resources can be accessed. The user cannot use the expected service.

You can use this command to configure the device to return an authentication failure packet to the 802.1X client or Portal server. In 802.1X authentication, the 802.1X client notifies the user of authentication failure. In Portal authentication, the Portal server pushes an authentication failure message to the user. The user then choose whether to perform reauthentication.

Precautions

- If the command is executed in both the interface view and system view, the configuration in interface view takes effect.
- This function takes effect only for users who go online after this function is successfully configured.
- This command is only applicable to the 802.1X authentication and Portal authentication.

Example

Configure GE0/0/1 to return an authentication failure packet to the 802.1X client or Portal server when a user fails in authentication.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication event authen-fail response-fail
```

13.6.16 authentication event session-timeout

Function

The **authentication event session-timeout** command sets the timeout period of network access rights granted to users in different authentication stages.

The **undo authentication event session-timeout** command restores the default timeout period.

By default, the timeout period of network access rights granted to users is 15 minutes.

Format

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

authentication event { **pre-authen** | **authen-fail** | **authen-server-down** | **client-no-response** } **session-timeout** *session-time*

undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** | **client-no-response** } **session-timeout**

VLANIF interface view

authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } **session-timeout** *session-time*

undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } **session-timeout**

Parameters

Parameter	Description	Value
pre-authen	Specifies the timeout period of the network access rights granted to users before authentication starts.	-
authen-fail	Specifies the timeout period of the network access rights granted to users when authentication fails.	-
authen-server-down	Specifies the timeout period of the network access rights granted to users when the authentication server does not respond.	-
client-no-response	Specifies the timeout period of the network access rights granted to users when the 802.1X client does not respond. This parameter is only valid for 802.1X authentication.	-
session-time	Specifies the value of timeout period. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.	The value is an integer that ranges from 0 to 71581, in minutes.

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **authentication event** command to grant the network access rights to users in different authentication stages, you can run the **authentication event session-timeout** command to specify the timeout period for the network access rights. Users can access the authorized resources within the timeout period, and will be forced to go offline after the timeout period expires.

If the aging time is set to 0, the network access rights granted to the user will not expire. To disconnect the user from the network, run the **cut access-user** command on the device or configure the authentication server to deliver an offline message to the user.

Precautions

The timeout period set in the VLANIF interface view is not applicable to 802.1X authentication.

If this command is only run in the system view, the configuration takes effect on all interfaces. If this command is run in both the system view and interface view, the configuration on interfaces takes precedence over the global configuration.

This function takes effect only for users who go online after this function is successfully configured.

Example

On interface GE0/0/1, set the timeout period of the network access rights granted to users when authentication fails to 100 minutes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication event authen-fail session-timeout 100
```

13.6.17 authentication guest-vlan

Function

The **authentication guest-vlan** command configures a guest VLAN on an interface.

The **undo authentication guest-vlan** command deletes a guest VLAN from an interface.

By default, no guest VLAN is configured on an interface.

Format

In the system view:

authentication guest-vlan *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication guest-vlan [*vlan-id*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication guest-vlan *vlan-id*

undo authentication guest-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a guest VLAN.	The value is an integer that ranges from 1 to 4094.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During 802.1X authentication and MAC address authentication, a guest VLAN allows users to access limited resources without authentication. The device supports the guest VLAN function.

Users in the guest VLAN can access resources in the guest VLAN without authentication but must be authenticated when they access external resources.

NOTE

- The restrict VLAN is for the users who fail the authentication, while the guest VLAN is for the users who are not authenticated.
- If only a guest VLAN is configured but no restrict VLAN is configured, the users who fail the authentication are added to the guest VLAN.

Prerequisites

The VLAN to be configured as the guest VLAN must have been created.

802.1X authentication has been enabled globally and on the interface using the **dot1x enable** command, or MAC address authentication has been enabled globally and on the interface using the **mac-authen** command.

Precautions

- The guest VLAN function can take effect only in 802.1X and MAC address authentication.
- A super VLAN cannot be configured as a guest VLAN.
- When free IP subnets are configured, the guest VLAN function becomes invalid immediately.
- The guest VLAN function takes effect only when a user sends untagged packets to the device.
- Different interfaces can be configured with different guest VLANs. After a guest VLAN is configured on an interface, the guest VLAN cannot be deleted.
- To make the VLAN authorization function take effect, the link type and access control mode of the authentication interface must meet the following requirements:
  - When the link type is hybrid in untagged mode, the access control mode can be based on the MAC address or interface.
  - When the link type is access or trunk, the access control mode can only be based on the interface.

Example

In the system view, configure 802.1X authentication for the users using Port-based access method on GE0/0/1 and set the guest VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] dot1x enable interface gigabitethernet 0/0/1
[HUAWEI] dot1x port-method port interface gigabitethernet 0/0/1
[HUAWEI] authentication guest-vlan 20 interface gigabitethernet 0/0/1
```

In the interface view, enable MAC address authentication on GE0/0/1 and set the guest VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] mac-authen
```



```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] mac-authen
[HUAWEI-GigabitEthernet0/0/1] authentication guest-vlan 20
```

13.6.18 authentication mac-move enable

Function

The **authentication mac-move enable** command enables MAC address migration.

The **undo authentication mac-move enable** command disables MAC address migration.

By default, MAC address migration is disabled.

Format

authentication mac-move enable vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1–10> }

undo authentication mac-move enable vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1–10> }

Parameters

Parameter	Description	Value
vlan	Specifies the VLAN range for enabling MAC address migration.	-
all	Enables MAC address migration in all VLANs.	-
vlan-id1 [**to** *vlan-id2*]	Enables MAC address migration in the specified VLANs. • *vlan-id1* specifies the ID of the first VLAN. • *vlan-id2* specifies the ID of the second VLAN. The value of *vlan-id2* must be greater than that of *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user is authenticated and accesses the network from one interface of the device, the network cable is pulled out from the interface and plugged in another interface on the device, then the user cannot immediately initiate authentication and access the network. The user can initiate authentication on the current interface only after the user offline detection interval expires or the authentication interface is manually enabled and shut down to clear user online entries. To improve user experience, MAC address migration is enabled so that the user can immediately initiate authentication and access the network after be switched to another access interface.

MAC address migration allows online NAC authentication users to immediately initiate authentication and access the network after they are switched to other access interfaces. If the user is authenticated successfully on the new interface, the online user entry on the original interface is deleted immediately to ensure that only one interface records the online user entry.

In addition, VLANs need to be specified for users in MAC address migration. The VLANs before and after the migration can be specified for the users, and they can be the same or different.

Precautions

- In normal case, enabling MAC address migration is not recommended. It should be enabled only when users have migration requirements during roaming. This prevents unauthorized users from forging MAC addresses of online users and sending ARP, 802.1X, or DHCP packets on other authentication control interfaces to trigger the MAC address migration function and force authorized user offline.
- Cascading migration through intermediate devices is not supported, because ARP and DHCP packets are not sent after the cascading migration.
- MAC address migration is not supported for Layer 3 Portal authentication users.
- In the Layer 2 BNG scenario, the device does not support MAC address migration.
- A user is switched from an interface configured with NAC authentication to another interface not configured with NAC authentication. In this case, the user can access the network only after the original online entry is aged because the new interface cannot send authentication packets to trigger MAC migration.
- In common mode, Portal authentication is triggered only after users who go online through a VLANIF interface send ARP packets and go offline; otherwise, the users can go online again only after the original user online entries age out. Portal authentication cannot be triggered after users who go online through physical interfaces migrate. The users can go online again only after the original user online entries age out.

- After a user who goes online from a VLANIF interface is quieted because of multiple MAC address migrations, MAC address migration can be performed for the quieted user only after the quiet period expires and the ARP entry is aged out.
- When an authorized VLAN is specified in the **authentication mac-move enable vlan** command, you are advised to enable the function of detecting the user status before user MAC address migration.

Example

Enable MAC address migration in all VLANs.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move enable vlan all
```

13.6.19 authentication mac-move detect enable

Function

The **authentication mac-move detect enable** command enables a device to detect users' online status before user MAC address migration.

The **undo authentication mac-move detect enable** command disables a device from detecting users' online status before user MAC address migration.

By default, a device is disabled from detecting users' online status before user MAC address migration.

Format

authentication mac-move detect enable

undo authentication mac-move detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To prevent unauthorized users from spoofing online users to attack a device, run the **authentication mac-move detect enable** command to enable the device to detect users' online status before user MAC address migration. If no users are online, the device permits MAC address migration and allows users to go online from a new access interface. If a user is online, the device terminates MAC address migration and does not allow the user to go online from a new access interface.

You can also run the **authentication mac-move detect retry-interval retry-time** command to set the detection interval and maximum number of detections before user MAC address migration.

Example

Enable a device to detect users' online status before user MAC address migration.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move detect enable
```

13.6.20 authentication mac-move detect retry-interval retry-time

Function

The **authentication mac-move detect retry-interval retry-time** command sets the detection interval and maximum number of detections before user MAC address migration.

The **undo authentication mac-move detect retry-interval retry-time** command restores the default setting.

By default, a device detects users' online status once. The detection interval is 3 seconds.

Format

authentication mac-move detect { **retry-interval** *interval* | **retry-time** *times* } *

undo authentication mac-move detect { **retry-interval** | **retry-time** } *

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a device detects users' online status before user MAC address migration.	The value is an integer that ranges from 1 to 5, in seconds.
times	Specifies the maximum number of detections before user MAC address migration.	The value is an integer that ranges from 1 to 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a device is enabled to detect users' online status before user MAC address migration, you can run the **authentication mac-move detect** { **retry-interval** *interval* | **retry-time** *times* } * command to modify the default detection interval and maximum number of detections.

Example

Configure a device to detect users' online status twice at an interval of 5 seconds before user MAC address migration.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move detect retry-interval 5 retry-time 2
```

13.6.21 authentication mac-move quiet-log enable

Function

The **authentication mac-move quiet-log enable** command enables the device to record logs about MAC address migration quiet.

The **undo authentication mac-move quiet-log enable** command disables the device from recording logs about MAC address migration quiet.

By default, the device is enabled to record logs about MAC address migration quiet.

Format

authentication mac-move quiet-log enable

undo authentication mac-move quiet-log enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can record logs when adding or deleting MAC address migration quiet entries. This helps the administrator to find out the cause for MAC address

migration failure, and improves maintainability of the MAC address migration quiet function.

Example

Enable the device to record logs about MAC address migration quiet.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-log enable
```

13.6.22 authentication mac-move quiet-times quiet-period

Function

The **authentication mac-move quiet-times quiet-period** command configures the quiet period and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state.

The **undo authentication mac-move quiet-times quiet-period** command restores the default settings.

The default quiet period is 0 seconds and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state is 3.

Format

authentication mac-move { **quiet-times** *times* | **quiet-period** *quiet-value* } *

undo authentication mac-move { **quiet-times** | **quiet-period** } *

Parameters

Parameter	Description	Value
times	Specifies the maximum number of MAC address migration times within 60 seconds before users enter the quiet state.	The value is an integer that ranges from 1 to 10.
quiet-value	Specifies the quiet period for MAC address migration users.	The value is an integer that ranges from 0 to 3600. The value 0 indicates that the MAC address migration quiet function is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When users frequently switch access interfaces (especially frequent switching due to loops), the device needs to process a large number of authentication packets and entries, which results in high CPU usage. To solve this problem, configure the MAC address migration quiet function.

If the number of MAC address migration times for a user within 60 seconds exceeds the value (*times*) after the MAC address migration quiet function is enabled, the device quiets the user for a certain period (*quiet-value*). During the quiet period, the device does not allow users to perform MAC address migration.

Example

Configure the quiet period to 120 seconds and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state to 5.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-times 5 quiet-period 120
```

13.6.23 authentication mac-move quiet-user-alarm enable

Function

The **authentication mac-move quiet-user-alarm enable** command enables the device to send alarms about MAC address migration quiet.

The **undo authentication mac-move quiet-user-alarm enable** command disables the device from sending alarms about MAC address migration quiet.

By default, the device is disabled from sending alarms about MAC address migration quiet.

Format

authentication mac-move quiet-user-alarm enable

undo authentication mac-move quiet-user-alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can send alarms about MAC address migration quiet to improve maintainability of the MAC address migration quiet function. The device sends alarms when the percentage of the actual user amount in the MAC address migration quiet table against the maximum number of users exceeds the upper alarm threshold configured. If the percentage decreases to be equal to or smaller than the lower alarm threshold, the device sends a clear alarm. The upper and lower alarm thresholds are configured using the **authentication mac-move quiet-user-alarm percentage** command.

Example

Enable the device to send alarms about MAC address migration quiet.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-user-alarm enable
```

13.6.24 authentication mac-move quiet-user-alarm percentage

Function

The **authentication mac-move quiet-user-alarm percentage** command configures the upper and lower alarm thresholds for the percentage of MAC address migration users in quiet state.

The **undo authentication mac-move quiet-user-alarm percentage** command restores the default setting.

By default, the lower alarm threshold is 50 and upper alarm threshold is 100.

Format

authentication mac-move quiet-user-alarm percentage *lower-threshold upper-threshold*

undo authentication mac-move quiet-user-alarm percentage

Parameters

Parameter	Description	Value
lower-threshold	Specifies the lower alarm threshold.	The value is an integer that ranges from 1 to 100.
upper-threshold	Specifies the upper alarm threshold.	The value is an integer that ranges from 1 to 100. The value must be greater than that of *lower-threshold*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **authentication mac-move quiet-user-alarm enable** command can be run to enable the device to send alarms about MAC address migration quiet to improve maintainability of the MAC address migration quiet function. The device sends alarms when the percentage of the actual user amount in the MAC address migration quiet table against the maximum number of users exceeds the upper alarm threshold configured. If the percentage decreases to be equal to or smaller than the lower alarm threshold, the device sends a clear alarm. The upper and lower alarm thresholds are configured using the **authentication mac-move quiet-user-alarm percentage** command.

Precautions

When a user goes online at a rate exceeding the upper limit, the alarm may not be generated.

Example

Configure the upper alarm threshold to 80 and lower alarm threshold to 40.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-user-alarm percentage 40 80
```

13.6.25 authentication max-reauth-req

Function

The **authentication max-reauth-req** command sets the maximum number of re-authentication attempts for users in a critical VLAN.

The **undo authentication max-reauth-req** command restores the default setting.

By default, the maximum number of re-authentication attempts is 20 for users in a critical VLAN.

Format

In the system view:

authentication max-reauth-req *times* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication max-reauth-req [*times*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication max-reauth-req *times*

undo authentication max-reauth-req [*times*]

Parameters

Parameter	Description	Value
times	Specifies the maximum number of re-authentication attempts.	The value is an integer that ranges from 1 to 20. The default value is 20.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *Interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

When the authentication server maintained by the device turns to the Up state, the device triggers re-authentication for users already added to the critical VLAN. If the authentication is successful, the users exit the critical VLAN. However, if the re-authentication fails due to reasons such as the fault of the access user's client, the repeated re-authentication degrades the device performance. After the maximum number of re-authentication attempts is set for users in the critical VLAN, the device forces the user to exit the critical VLAN if the user fails the authentication the specified number of times.

Example

Set the maximum number of re-authentication attempts for users in the critical VLAN to 5 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] authentication max-reauth-req 5 interface gigabitethernet 0/0/1
```


13.6.26 authentication open

Function

The **authentication open** command enables the NAC open function.

The **undo authentication open** command disables the NAC open function.

By default, the NAC open function is disabled on an interface.

Format

In the system view:

authentication open interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication open interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication open

undo authentication open

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a new NAC network is set up, the network administrator should pay attention to the number of potential access users and authentication method but does not need to control user access, because the administrator needs to configure user names, passwords, and authorization information on the authentication server. After 802.1X or MAC address authentication is configured on the access device, only authenticated users can access the network, so the administrator cannot obtain information about the users who do not have user names and passwords on the authentication server.

The NAC open function allows the users who failed in authentication to access the network.

Precautions

- The NAC open function is only applied to 802.1X and MAC address authentication.
- The NAC open function is only applied to RADIUS remote authentication.
- The NAC open function is valid only when the MAC address-based mode is used as the access control mode of the interface. After this function is enabled, users can be added to VLANs except a guest VLAN after they log in.
- After NAC open is enabled on an interface and fixed user names are used for MAC address authentication, the users on the interface are allowed to access the network even if they have used incorrect user names or passwords.

Example

Enable the NAC open function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] authentication open interface gigabitethernet 0/0/1
```

13.6.27 authentication port-vlan-modify user-online

Function

The **authentication port-vlan-modify user-online** command enables the function of keeping users online when the port type or VLAN is changed.

The **undo authentication port-vlan-modify user-online** command restores the default setting.

By default, the function of keeping users online when the port type or VLAN is changed is disabled.

Format

authentication port-vlan-modify user-online

undo authentication port-vlan-modify user-online

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After user access authentication succeeds, you can change the VLAN allowed to access or the access interface type through the RADIUS server. For example, you can assign VLANs to clients through the server for network planning and deployment. After the deployment is complete, to reduce the impact of link faults and device restart on the network and implement rapid network restoration, you can change the user access VLAN to the authorized VLAN. In this case, you can enable the function of keeping users online when the port type or VLAN is changed to modify interface or VLAN configurations.

Precautions

This function is only supported by MAC and 802.1X authentication.

This function is only supported by wired users.

Example

Enable the function of keeping users online when the port type or VLAN is changed.

```
<HUAWEI> system-view
[HUAWEI] authentication port-vlan-modify user-online
```

13.6.28 authentication restrict-vlan

Function

The **authentication restrict-vlan** command configures a restrict VLAN on an interface.

The **undo authentication restrict-vlan** command deletes the restrict VLAN from an interface.

By default, no restrict VLAN is configured on an interface.

Format

In the system view:

authentication restrict-vlan *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication restrict-vlan [*vlan-id*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication restrict-vlan *vlan-id*

undo authentication restrict-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a restrict VLAN.	The value is an integer that ranges from 1 to 4094.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the restrict VLAN on the device interface, so that the users can still access some network resources (for example, update the virus library) when the users fail the authentication. The users who fail the authentication are added to the restrict VLAN to access the resources in the restrict VLAN. Note that, the user fails the authentication because the authentication server rejects the user for some reasons, for example, the user enters an incorrect user password, not because the authentication times out or the network is disconnected.

NOTE

- The restrict VLAN is for the users who fail the authentication, while the guest VLAN is for the users who are not authenticated.
- If only a guest VLAN is configured but no restrict VLAN is configured, the users who fail the authentication are added to the guest VLAN.

Prerequisites

The VLAN to be configured as the restrict VLAN must have been created.

Precautions

- A super VLAN cannot be configured as a restrict VLAN.
- When free IP subnets are configured, the restrict VLAN function becomes invalid immediately.
- The restrict VLAN function takes effect only when a user sends untagged packets to the device.
- To make the VLAN authorization function take effect, the link type and access control mode of the authentication interface must meet the following requirements:
  - When the link type is hybrid in untagged mode, the access control mode can be based on the MAC address or interface.
  - When the link type is access or trunk, the access control mode can only be based on the interface.

Example

In the system view, configure 802.1X authentication for the users using Port-based access method on GE0/0/1 and set the restrict VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] dot1x enable interface gigabitethernet 0/0/1
[HUAWEI] dot1x port-method port interface gigabitethernet 0/0/1
[HUAWEI] authentication restrict-vlan 20 interface gigabitethernet 0/0/1
```

13.6.29 authentication speed-limit auto

Function

The **authentication speed-limit auto** command enables the device to dynamically adjust the rate of packets from NAC users.

The **undo authentication speed-limit auto** command disables the device from dynamically adjusting the rate of packets from NAC users.

By default, the device does not dynamically adjust the rate of packets from NAC users.

Format

authentication speed-limit auto

undo authentication speed-limit auto

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a lot of NAC users send authentication or log off requests to the device, the CPU usage may be overloaded especially when the CPU or memory usage is already high (for example, above 80%).

After this command is executed, the device limits the number of NAC packets received per second if the CPU or memory usage is high. This function reduces loads on the device CPU.

Example

Enable the device to dynamically adjust the rate of packets from NAC users.

```
<HUAWEI> system-view
[HUAWEI] authentication speed-limit auto
```

13.6.30 authentication timer re-authen

Function

The **authentication timer re-authen** command configures the interval for re-authenticating pre-connection users or users who fail to be authenticated.

The **undo authentication timer re-authen** command restores the default setting.

By default, pre-connection users and users who fail to be authenticated are re-authenticated at an interval of 60 seconds.

Format

authentication timer re-authen { **pre-authen** *re-authen-time* | **authen-fail** *re-authen-time* }

undo authentication timer re-authen { **pre-authen** | **authen-fail** }

Parameters

Parameter	Description	Value
pre-authen *re-authen-time*	Specifies the interval for re-authenticating pre-connection users.	The value is an integer that ranges from 0 or 30 to 7200, in seconds. The value **0** indicates that the re-authentication function is disabled for pre-connection users.
authen-fail *re-authen-time*	Specifies the interval for re-authenticating users who fail to be authenticated.	The value is an integer that ranges from 30 to 7200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device creates the mapping user entries when network access policies are assigned to users who are in the pre-connection phase or fail authentication. To enable users to pass authentication in real time, the device periodically re-authenticates the users who are in the pre-connection phase or fail authentication according to the user entries. The administrator can adjust the re-authentication interval based on the actual network requirements.

Precautions

This command only applies to 802.1X authentication and MAC address authentication.

This function takes effect only for users who go online after this function is successfully configured.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

Configures the interval for re-authenticating users who fail to be authenticated to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication timer re-authen authen-fail 300
```


13.6.31 authentication user-alarm percentage

Function

The **authentication user-alarm percentage** command sets alarm thresholds for the percentage of successfully authenticated NAC users.

The **undo authentication user-alarm** command restores the default alarm thresholds for the percentage of successfully authenticated NAC users.

By default, the lower alarm threshold for the percentage of successfully authenticated NAC users is 50, and the upper alarm threshold is 100.

Format

authentication user-alarm percentage *percent-lower-value percent-upper-value*

undo authentication user-alarm

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of successfully authenticated NAC users.	The value is an integer in the range from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of successfully authenticated NAC users.	The value is an integer in the range from 1 to 100, and must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the number of successfully authenticated NAC users reaches a specified percentage, the device generates an alarm. You can run the **authentication user-alarm percentage** command to set the upper and lower alarm thresholds for this percentage.

When the percentage of successfully authenticated NAC users against the maximum number of users allowed by the device is greater than or equal to the upper alarm threshold, the device generates an alarm. When this percentage reaches or falls below the lower alarm threshold, the device generates a clear alarm.

Example

Set the lower and upper alarm thresholds for the percentage of successfully authenticated NAC users to 30 and 80, respectively.

```
<HUAWEI> system-view
[HUAWEI] authentication user-alarm percentage 30 80
```

13.6.32 band-width share-mode

Function

The **band-width share-mode** command enables the bandwidth share mode.

The **undo band-width share-mode** command restores the default configuration.

By default, the bandwidth share mode is disabled.

NOTE

This command is only supported by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

band-width share-mode

undo band-width share-mode

Parameters

None

Views

System view, AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On a home network, all family members go online using the same account. To improve service experience of family members, you can enable the bandwidth share mode so that all members can share the bandwidth.

Precautions

- If this command is run in the system view, it takes effect for all new online users who connected to the device. If this command is run in the AAA domain view, it takes effect only for new online users in the domain.
- If the local or remote RADIUS server does not assign CAR settings to the users who will go online and the online users, the share mode is invalid to the users.

- If the bandwidth share mode is enabled and different users use the same account for authentication, the users going online with no CAR settings assigned will not be affected when CAR settings are assigned to the users who go online later.

Example

Enable the bandwidth share mode in the system view.

```
<HUAWEI> system-view
[HUAWEI] band-width share-mode
```

Enable the bandwidth share mode in the AAA domain view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] band-width share-mode
```

13.6.33 car (user group view)

Function

The **car** command enables traffic control for users in a user group.

The **undo car** command disables traffic control for users in a user group.

By default, traffic control is disabled for users in a user group.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command, and the user group CAR can only be applied in the interface outbound direction (**outbound**) on the S6720-EI, S6720S-EI.

Format

car { **outbound** | **inbound** } **cir** *cir-value* [**pir** *pir-value* | **cbs** *cbs-value* | **pbs** *pbs-value*] *

undo car { **outbound** | **inbound** }

Parameters

Parameter	Description	Value
outbound	Applies the user group CAR to the outgoing packets on an interface to restrict the outgoing packet rate.	-

Parameter	Description	Value
inbound	Applies the user group CAR to the incoming packets on an interface to restrict the incoming packet rate.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The PIR value must be greater than or equal to the CIR value. The default PIR value is equal to the CIR value.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 10000 to 4294967295, in bytes. The default value of *cbs-value* is 188 x *cir-value*.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 10000 to 4294967295, in bytes. The value of *pbs-value* must be larger than that of *cbs-value* and is equal to 188 times of the value of *pir-value* by default.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After user groups are created using the **user-group** command, you can run the **car outbound** command to configure traffic control for users in a user group so that users in different groups are allocated different bandwidths.

Precautions

- The **car** command takes effect on each user in a user group.
- This function takes effect only for users who go online after this function is successfully configured.

Example

Set the CIR to 10000 Kbit/s and the CBS to 50000 bytes for outgoing packets of users in a user group.

```
<HUAWEI> system-view
[HUAWEI] user-group test
[HUAWEI-user-group-test] car outbound cir 10000 cbs 50000
```

13.6.34 cut access-user

Function

The **cut access-user** command forces users offline.

Format

cut access-user open

cut access-user user-group *group-name*

Parameters

Parameter	Description	Value
open	Forces open users offline.	-
user-group *group-name*	Specifies the user group based on which the users are forced offline.	The value must be an existing user group name.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

After a user goes online, if you want to modify the user's network access rights or detect that the user is unauthorized, run this command to force the user offline.

Example

Force open users offline.


```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] cut access-user open
```

13.6.35 display aaa statistics access-type-authenreq

Function

The **display aaa statistics access-type-authenreq** command displays the number of requests for MAC, Portal, or 802.1X authentication.

Format

display aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, or 802.1X authentications.

To view the number of requests for MAC, Portal, or 802.1X authentication, run the **display aaa statistics access-type-authenreq** command.

Example

Display the number of requests for MAC, Portal, or 802.1X authentication.

```
<HUAWEI> display aaa statistics access-type-authenreq
mac     authentication request     :2
portal  authentication request     :0
dot1x   authentication request     :0
```

Table 13-95 Description of the **display aaa statistics access-type-authenreq** command output

Item	Description
mac authentication request	Number of MAC authentication requests.
portal authentication request	Number of Portal authentication requests.

Item	Description
dot1x authentication request	Number of 802.1X authentication requests.

13.6.36 display authentication mode

Function

The **display authentication mode** command displays the current NAC configuration mode and the mode after restart.

Format

display authentication mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display authentication mode** command to view the current NAC configuration mode.

Example

Display the current NAC configuration mode and the mode after restart.

```
<HUAWEI> display authentication mode
  Current authentication mode is unified-mode
  Next authentication mode is unified-mode
```

Table 13-96 Description of the **display authentication mode** command output

Item	Description
Current authentication mode is unified-mode	Current NAC configuration mode.

Item	Description
Next authentication mode is unified-mode	NAC configuration mode after the device restarts. Run the **authentication unified-mode** command to switch the NAC mode to unified mode. Run the **undo authentication unified-mode** command to switch the NAC mode to common mode.

13.6.37 display access-user

Function

The **display access-user** command displays information about online NAC users.

Format

display access-user open

display access-user option82 { **circuit-id** *text* | **remote-id** *text* }

display access-user user-group *group-name* [**detail**]

NOTE

The **detail** parameter is only supported by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Parameters

Parameter	Description	Value
open	Displays open user information.	-
option82	Displays information about MAC address authentication users who use the Option 82 field as user names.	-
circuit-id *text*	Displays information about MAC address authentication users who specify the circuit ID as user names.	The value must be existing circuit-id information.

Parameter	Description	Value
remote-id *text*	Displays information about MAC address authentication users who specify the remote ID as user names.	The value must be existing remote-id information.
user-group *group-name*	Displays information about users in a specified user group.	The value must be an existing user group index.
detail	Displays detailed information about users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about online NAC users.

Example

Display open user information.

```
<HUAWEI> display access-user open
------------------------------------------------------------------------------
UserID Username              IP address       MAC            Status
------------------------------------------------------------------------------
16016  1@radius              10.8.7.5         00e0-fc12-3456 Success
------------------------------------------------------------------------------
Total: 1, printed: 1, Open: 1, printed: 1
```

NOTE

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

When you run the **display access-user** command without specifying any parameter to view user information and the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following the 19th character; that is, only 22 characters are displayed. When you run the **display access-user** command with parameters specified to view detailed information about the user table, all the characters of **username** are displayed, and the rule for converting special characters remains unchanged.

Display detailed information about users in user group 1.

```
<HUAWEI> display access-user user-group 1 detail
------------------------------------------------------------------------------
```



```
Basic:
  User ID                    : 114
  User name                  : lx
  Domain-name                : lx
  User MAC                   : 00e0-fc01-0105
  User IP address            : 10.1.1.5
  User vpn-instance          : -
  User IPv6 address          : -
  User access Interface      : GigabitEthernet0/0/5
  User vlan event            : Success
  QinQVlan/UserVlan          : 0/200
  User vlan source           : user request
  User access time           : 2015/02/08 14:35:02
  User accounting session ID  :
5735_S0000500000020072****0000072
  Option82 information       : -
  User access type           : MAC
  Terminal Device Type       : Data Terminal
  Dynamic group name(Effective)  : 1
  Session Timeout            : 1800(s) (local), Remaining: 330(s)
  Termination Action         : RE-AUTHENTICATION
  Service Scheme Priority    : 0

AAA:
  User authentication type   : MAC authentication
  Current authentication method  : None
  Current authorization method   : -
  Current accounting method      : None

 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```

Table 13-97 Description of the display access-user command output

Item	Description
UserID/User ID	ID that is assigned to a user after the user goes online.
Username/User name	User name.
IP address	User IP address.
MAC	User MAC address.

Item	Description
Status,User vlan event	User access status. • Open: For a wired user, the user goes online through the open function upon authentication failure. For wireless users, no authentication is performed. • Success: authentication is successful • Pre-authen: pre-authentication • Client-no-resp: the client does not respond • Fail-authorized: authorization upon authentication failure • Web-server-down: web server is Down • Aaa-server-down: AAA server is Down
Domain-name	User domain.
User MAC	User MAC address.
User IP address	User IP address.
User vpn-instance	VPN instance to which the user belongs.
User IPv6 address	User IPv6 address.
User access Interface	User access interface.
QinQVlan/UserVlan	VLAN to which the user belongs. • In QinQ application, **QinQVlan** indicates the outer VLAN ID, and **UserVlan** indicates the inner VLAN ID. • For a common VLAN, **UserVlan** indicates the VLAN to which the user belongs, and the value of **QinQVlan** is 0.

Item	Description
User vlan source	Source of the user VLAN. • server vlan: The VLAN is delivered by the remote server. • user group vlan: the VLAN is bound to a user group. • service scheme vlan: The VLAN is configured in the service scheme view. • local event vlan: The VLAN is a locally configured authorized VLAN (for guests or NAC escape). • user request: The VLAN is carried in the user authentication request.
User access time	Time when a user goes online. If the system is configured with a time zone and uses DST, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.
User accounting session ID	ID of an accounting session.
Option82 information	Option 82 information.
User access type	User access type: **IPoE** indicates an IP session user.
Terminal Device Type	Terminal device type.
Dynamic group name(Effective)	Name of a UCL group.
Session Timeout	Session timeout period. • xx(s) (local): indicates the locally configured reauthentication interval for MAC or 802.1X authentication users. • xx(s) (server): indicates that the RADIUS server delivers the Session-Timeout (27) attribute, which indicates the maximum number of seconds a user should be allowed to remain connected.

Item	Description
Termination Action	Whether the device is configured to reauthenticate users when the time exceeds the value of Session-Timeout delivered by the RADIUS server. • reauthenticate: Reauthentication is performed. To configure this function, run the **authentication termination-action reauthenticate** command.
Service Scheme Priority	User priority in a service scheme.
AAA	AAA information of the user.
User authentication type	User authentication type, which depends on the access type of the user.
Current authentication method	Current authentication mode.
Current authorization method	Current authorization mode.
Current accounting method	Current accounting mode.
Total	Total number of online users.
printed	Number of displayed online users.

13.6.38 display access-user dot1x-identity statistics

Function

The **display access-user dot1x-identity statistics** command displays statistics about Identity packets for 802.1X authentication on a switch.

Format

display access-user dot1x-identity statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view the statistics about Identity packets for 802.1X authentication on a switch.

Example

Display statistics about Identity packets for 802.1X authentication on the switch.

```
<HUAWEI> display access-user dot1x-identity statistics
------------------------------------------------------------------------
Receive(Packet)    Pass(Packet)    Drop(Packet)    Last-dropping-time
------------------------------------------------------------------------
0                  0               0               -
------------------------------------------------------------------------
```

Table 13-98 Description of the **display access-user dot1x-identity statistics** command output

Item	Description
Receive(Packet)	Total number of Identity packets for 802.1X authentication received by the switch.
Pass(Packet)	Number of Identity packets for 802.1X authentication sent to and processed by the CPU of the switch.
Drop(Packet)	Number of Identity packets for 802.1X authentication discarded by the switch.
Last-dropping-time	Latest time when the switch discarded Identity packets for 802.1X authentication. If no packet loss record exists on the switch, this field displays -.

13.6.39 display authentication mac-move configuration

Function

The **display authentication mac-move configuration** command displays the MAC address migration configuration.

Format

display authentication mac-move configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display authentication mac-move configuration** command to view the MAC address migration configuration. The configuration includes the number of times that MAC address migration users are allowed to migrate their MAC addresses 60s before they enter the quiet state, the period that MAC address migration users stay in the quiet state, the interval at which a device detects users' online status before user MAC address migration, and the number of detections before user MAC address migration.

Example

Display the MAC address migration configuration.

```
<HUAWEI> display authentication mac-move configuration
Mac-move vlan config:all
Mac-move quiet times:1
Mac-move quiet period(s):120
Mac-move quiet log:ENABLE
Mac-move quiet user alarm:ENABLE
Mac-move quiet user alarm lower percentage(%):
50
Mac-move quiet user alarm upper percentage(%):100
Mac-move detect:DISABLE
Mac-move detect retry-interval(s):3
Mac-move detect retry-time:1
```

Table 13-99 Description of the **display authentication mac-move configuration** command output

Item	Description
Mac-move vlan config	VLAN ID range in which MAC address migration is enabled. For details, see the **authentication mac-move enable** command.
Mac-move quiet times	Number of times that MAC address migration users are allowed to migrate their MAC addresses 60s before they enter the quiet state. For details, see the **authentication mac-move quiet-times quiet-period** command.

Item	Description
Mac-move quiet period(s)	Period that MAC address migration users stay in the quiet state. For details, see the **authentication mac-move quiet-times quiet-period** command.
Mac-move quiet log	Whether a device is enabled to record logs about user quietness triggered by MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move quiet-log enable** command.
Mac-move quiet user alarm	Whether a device is enabled to send alarms about user quietness triggered by MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move quiet-user-alarm enable** command.
Mac-move quiet user alarm lower percentage(%)	Lower alarm threshold for the percentage of MAC address migration users in quiet state. For details, see the **authentication mac-move quiet-user-alarm percentage** command.
Mac-move quiet user alarm upper percentage(%)	Upper alarm threshold for the percentage of MAC address migration users in quiet state. For details, see the **authentication mac-move quiet-user-alarm percentage** command.
Mac-move detect	Whether a device is enabled to detect users' online status before user MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move detect enable** command.

Item	Description
Mac-move detect retry-interval(s)	Interval at which a device detects users' online status before user MAC address migration. For details, see the **authentication mac-move detect retry-interval retry-time** command.
Mac-move detect retry-time	Number of detections before user MAC address migration. For details, see the **authentication mac-move detect retry-interval retry-time** command.

13.6.40 display authentication mac-move quiet-user

Function

The **display authentication mac-move quiet-user** command displays information about MAC address migration users in quiet state.

Format

display authentication mac-move quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all MAC address migration users in quiet state.	-
mac-address *mac-address*	Displays information about MAC address migration users in quiet state with a specified MAC address.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run this command to view information about MAC address migration users in quiet state.

Example

Display information about all MAC address migration users in quiet state.

```
<HUAWEI> display authentication mac-move quiet-user all
Quiet MAC Information
--------------------------------------------------------------------------------
Quiet MAC                                 Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
00e0-fc02-0003                             143
--------------------------------------------------------------------------------
1 quiet MAC found, 1 printed.
```

Table 13-100 Description of the **display authentication mac-move quiet-user all** command output

Item	Description
Quiet MAC	MAC address of MAC address migration users in quiet state.
Quiet Remain Time(Sec)	Remaining quiet time of MAC address migration users in quiet state, in seconds.

13.6.41 display authentication user-alarm configuration

Function

The **display authentication user-alarm configuration** command displays alarm thresholds for the percentage of successfully authenticated NAC users.

Format

display authentication user-alarm configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the alarm thresholds for the percentage of successfully authenticated NAC users.

Example

Display the alarm thresholds for the percentage of successfully authenticated NAC users.

```
<HUAWEI> display authentication user-alarm configuration
  Current Alarm Percent:100
  Current Alarm Resume Percent:60
```

Table 13-101 Description of the **display authentication user-alarm configuration** command output

Item	Description
Current Alarm Percent	Upper alarm threshold for the percentage of successfully authenticated NAC users.
Current Alarm Resume Percent	Lower alarm threshold for the percentage of successfully authenticated NAC users.

13.6.42 display dot1x

Function

The **display dot1x** command displays 802.1X authentication information.

Format

display dot1x statistics

display dot1x [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
statistics	Displays statistics on 802.1X authentication. The statistics about 802.1X authentication is displayed only when this parameter is specified.	-

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays 802.1X authentication information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. 802.1X authentication information on all device interfaces is displayed if this parameter is not specified.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display dot1x** command to view configuration results of all configuration commands in 802.1X authentication and statistics about 802.1X packets.

The command output helps you to check whether the current 802.1X authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

The **display dot1x** command displays the statistics on 802.1X packets. You can locate the fault according to the packet statistics. When the fault is rectified, run the **reset dot1x statistics** command to clear the packet statistics. After a period of time, run the **display dot1x** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

Display 802.1X authentication information.

```
<HUAWEI> display dot1x
 Global 802.1x is Enabled
 Authentication method is CHAP
 Max users: 1024
 Current users: 1
 DHCP-trigger is Disabled
 Handshake is Enabled
 Quiet function is Enabled
 Mc-trigger port-up-send is Disabled
 Parameter set:Dot1x Handshake Period       16s   Reauthen Period     60s
               Arp Handshake Period         0s   Client Timeout      10s
               Quiet Period               600s   Quiet-times         2
               Eth-Trunk Handshake Period   120s   Tx Period           30
               Mac-By-Pass Delay            30s
 Dot1x URL: www.***.com.cn
 Free-ip configuration(IP/mask):    192.168.1.0     /255.255.255.0
GigabitEthernet0/0/3 status: UP  802.1x protocol is Enabled
 Port control type is Auto
 Authentication mode is MAC-based
 Authentication method is CHAP
 Reauthentication is disabled
 Dot1x retry times: 2
 Authenticating users: 1
 Current users: 1

 Authentication Success: 1          Failure: 0
 Enter Enquence        : 0
 EAPOL Packets: TX     : 19         RX     : 0
 Sent      EAPOL Request/Identity Packets       : 1
           EAPOL Request/Challenge Packets      : 0
           Multicast Trigger Packets            : 18
           EAPOL Success Packets                : 0
           EAPOL Failure Packets                : 0
 Received  EAPOL Start Packets                  : 0
           EAPOL Logoff Packets                 : 0
           EAPOL Response/Identity Packets      : 0
           EAPOL Response/Challenge Packets     : 0

 Online user(s) info:
 UserId   MAC/VLAN           AccessTime             UserName
 ------------------------------------------------------------------------------
 17487    00e0-fc12-3456/34   2018/07/30 09:49:15     lss
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```

Display 802.1X statistics.

```
<HUAWEI> display dot1x statistics
 Dropped   EAPOL Access Flow Control       : 0
           EAPOL Check Sysmac Error        : 0
           EAPOL Get Vlan ID Error         : 0
           EAPOL Packet Flow Control       : 0
           EAPOL Online User Reach Max     : 0
```



```
        EAPOL Static or BlackHole Mac   : 0
        EAPOL Get Vlan Mac Error        : 0
        EAPOL Temp User Exist           : 0
        EAPOL no replace dot1x          : 0

DHCP    Enter Enqueue                     : 0
        Processed Packet                : 0
        Dropped Packet                  : 0

ARP     Enter Enqueue                     : 0
        Processed Packet                : 0
        Dropped Packet                  : 0

ND      Enter Enqueue                     : 0
        Processed Packet                : 0
        Dropped Packet                  : 0

DHCPv6  Enter Enqueue                     : 0
        Processed Packet                : 0
        Dropped Packet                  : 0

ANYL2   Enter Enqueue                     : 0
        Processed Packet                : 0
        Dropped Packet                  : 0

Sent    Authentication Request            : 0
        Cut Request                     : 0
        Cut Command Ack                 : 0
        Authentication Ack Fail Aff     : 0
        Update Ip                       : 0
        Wlan Eap Authentication Request   : 0
        Wlan Eap Authentication Request Ack  : 0
        Wlan Eap Send Pmk                 : 0
        Wlan Eap Reauthenticate Send Pmk  : 0
        Update User Online Time           : 0

Received  Authentication Ack              : 0
        Reauthenticate Command            : 0
        Cut Command                     : 0
        Cut Ack                         : 0
        Sam Nac Ack                     : 0
        Notify Server Up                : 0
        Wlan Eap Authentication Request   : 0
        Wlan Mac Authentication Request   : 0
        Notify Vlanif Mac Authentication  : 0
```

Table 13-102 Description of the **display dot1x** command output

Item	Description
Global 802.1x is Enabled	802.1X authentication is enabled globally. To enable 802.1X authentication, run the **dot1x enable** command.
Authentication method is CHAP	CHAP authentication is enabled. The authentication methods include EAP, CHAP, and PAP To enable CHAP authentication, run the **dot1x authentication-method** command.
Max users	Maximum number of global online users, the value varies according to device models. To set the maximum number of global online users, run the **dot1x max-user** command.

Item	Description
Current users	Number of current online users.
DHCP-trigger is Disabled	Authentication triggering through DHCP packets is disabled. To trigger authentication using DHCP packets, run the **dot1x dhcp-trigger** command.
Handshake is Enabled	The handshake function is enabled for online users.
Quiet function is Disabled	The quiet function is disabled for users. To enable the quiet function, run the **dot1x quiet-period** command.
Mc-trigger port-up-send is Disabled	The function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is disabled. To configure the function, run the **dot1x mc-trigger port-up-send enable** command.
Parameter set	Settings of 802.1X authentication parameters.
Dot1x Handshake Period	Handshake interval between the device and 802.1X authentication client connected to a non-Eth-Trunk interface. To set the handshake interval, run the **dot1x timer** command.
Reauthen Period	Re-authentication interval. To set the re-authentication interval, run the **dot1x timer** command.
Arp Handshake Period	Handshake interval of the device with pre-connection users and authorized users.
Client Timeout	Timeout interval of a client. To set the timeout interval of a client, run the **dot1x timer** command.
Quiet Period	Value of the quiet timer. To set the value of the quiet timer, run the **dot1x timer** command.
Quiet-times	Maximum number of authentication failures before an 802.1X user enters the quiet state. To set the maximum number of authentication failures, run the **dot1x quiet-times** command.

Item	Description
Eth-Trunk Handshake Period	Handshake interval between the device and 802.1X authentication client connected to an Eth-Trunk. To set the handshake interval, run the **dot1x timer** command.
Tx Period	The interval for sending authentication requests. To set the timeout interval of a client, run the **dot1x timer** command.
Mac-By-Pass Delay	The value of the delay timer for MAC address bypass authentication. To set the timeout interval of a client, run the **dot1x timer** command.
Dot1x URL	Redirect-to URL. To set the redirect-to URL, run the **dot1x url** command.
Free-ip configuration(IP/mask)	Free IP subnet. To set the free IP subnet, run the **dot1x free-ip** command.
GigabitEthernet0/0/1 state	State of an interface. ● UP: The interface is started. ● DOWN: The interface is shut down.
802.1x protocol is Enabled[mac-bypass]	802.1X authentication is enabled on the interface. To enable 802.1X authentication, run the **dot1x enable** command. To configure MAC address bypass authentication, run the **dot1x mac-bypass** command. If MAC address bypass authentication is configured, [mac-bypass] is displayed.
Port control type is Auto	The control mode on the interface is **auto** for 802.1X authentication user access. The access control modes include **auto**, **authorized-force**, and **unauthorized-force**. To set the control mode, run the **dot1x port-control** command.
Authentication mode is MAC-based	The MAC address-based authentication method is used on the interface. To set the authentication method on the interface, run the **dot1x port-method** command.
Reauthentication is disabled	802.1x user re-authentication is disabled on the interface. To enable 802.1X user re-authentication, run the **dot1x reauthenticate** command.

Item	Description
Dot1x retry times	Maximum number of times an authentication request is sent to an 802.1X user. To set the maximum number of times an authentication request is sent to an 802.1X user, run the **dot1x retry** command.
Authenticating users	Number of users who are being authenticated.
Current users	Number of current online users on the interface.
Authentication Success	Number of successful authentications. The statistics include statistics on online 802.1X users but not on the users using MAC address bypass authentication.
Failure	Number of failed authentications. The statistics include statistics on online 802.1X users but not on the users using MAC address bypass authentication.
Enter Enquence	Number of packets entering the queue.
EAPOL Packets	Number of globally EAPOL packets. • TX: Number of sent EAPOL packets. • RX: Number of received EAPOL packets.
Sent	Statistics of sent packet.
EAPOL Request/ Identity Packets	Number of globally EAPOL Request/Identity packets.
EAPOL Request/ Challenge Packets	Number of globally EAPOL Request/Challenge packets.
Multicast Trigger Packets	Number of multicast packets that trigger authentication.
EAPOL Success Packets	Number of globally EAPOL Success packets.
EAPOL Failure Packets	Number of globally EAPOL Failure packets.
Received	Statistics of received packet.
EAPOL Start Packets	Number of globally EAPOL Start packets.
EAPOL Logoff Packets	Number of globally EAPOL LogOff packets.
EAPOL Response/ Identity Packets	Number of globally EAPOL Response/Identity packets.

Item	Description
EAPOL Response/ Challenge Packets	Number of globally EAPOL Response/Challenge packets.
Online user(s) info	Online user information: ● UserId: User ID. ● MAC/VLAN: MAC address/VLAN ID. ● AccessTime: Access time. ● UserName: User name. ● Total: Total number of online users. ● printed: Number of displayed online users.
Dropped	Number of discarded EAP packets. ● EAPOL Access Flow Control: number of packets that are discarded because the user access rate is exceeded. ● EAPOL Check Sysmac Error: number of packets that are discarded because the device MAC address is incorrect. ● EAPOL Get Vlan ID Error: number of packets that are discarded because the obtained VLAN ID is incorrect. ● EAPOL Packet Flow Control: number of packets that are discarded because the packet access rate is exceeded. ● EAPOL Online User Reach Max: number of packets that are discarded because the number of online users reaches the maximum. ● EAPOL Static or BlackHole Mac: number of packets that are discarded because the packet MAC address is a static MAC address or blackhole MAC address. ● EAPOL Get Vlan Mac Error: number of packets that are discarded because the obtained VLAN MAC address is incorrect. ● EAPOL Temp User Exist: number of packets that are discarded because the temporary user exists. ● EAPOL no replace dot1x: number of EAP Start packets that are discarded due to 802.1X authentication of successfully authenticated MAC or Portal users.
DHCP	DHCP packet statistics.
ARP	ARP packet statistics.
ND	ND packet statistics.
DHCPv6	DHCPv6 packet statistics.
ANYL2	Any Layer 2 packet statistics.

Item	Description
Processed Packet	Number of processed packets.
Dropped Packet	Number of discarded packets.
Authentication Request	Number of authentication request messages.
Cut Request	Number of logout request messages.
Cut Command Ack	Number of acknowledgment messages to logout command request messages.
Authentication Ack Fail Aff	Number of the user is disconnected after the wireless user authentication fails.
Update Ip	Number of IP address update messages.
Wlan Eap Authentication Request	Number of EAP authentication request messages initiated by the WLAN module.
Wlan Eap Authentication Request Ack	Number of acknowledgment messages to EAP authentication request messages initiated by the WLAN module.
Wlan Eap Send Pmk	Number of PMK messages sent when the WLAN module performs EAP authentication.
Wlan Eap Reauthenticate Send Pmk	Number of PMK messages sent when the WLAN module performs EAP re-authentication.
Update User Online Time	Number of the user online time is updated.
Authentication Ack	Number of authentication acknowledgment messages.
Reauthenticate Command	Number of re-authentication messages.
Cut Command	Number of logout command request messages.
Cut Ack	Number of acknowledgment messages to logout request messages.
Sam Nac Ack	Number of EAP messages replied by the SAM module.
Notify Server Up	Number of RADIUS server Up messages.
Wlan Mac Authentication Request	Number of MAC authentication request messages initiated by the WLAN module.
Notify Vlanif Mac Authentication	Number of MAC authentication request messages of a VLANIF interface.

13.6.43 display dot1x quiet-user

Function

The **display dot1x quiet-user** command displays information about 802.1X authentication users who are quieted.

Format

display dot1x quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all 802.1X authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a quiet 802.1X authentication user with a specified MAC address.	The value is in H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about 802.1X authentication users who are quieted.

Example

Display information about all 802.1X authentication users who are quieted.

```
<HUAWEI> display dot1x quiet-user all
--------------------------------------------------------------------------------
MacAddress                User Status             Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
00e0-fc02-0003             Block                  50
--------------------------------------------------------------------------------
Total: 1  Printed: 1  Block: 1   Active: 0
```


Table 13-103 Description of the **display dot1x quiet-user all** command output

Item	Description
MacAddress	MAC address of an 802.1X authentication user who is quieted.
User Status	User status: • Block: The user is in silent state. • Active: The user is not in silent state.
Quiet Remain Time(Sec)	• If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. • If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.

13.6.44 display mac-address authen

Function

The **display mac-address authen** command displays the current authen MAC address entries in the system.

Format

display mac-address authen [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-

Parameter	Description	Value
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The authen MAC address entries are generated for pre-connection users or after users pass authentication. The administrator can run this command to check the existing authen or guest MAC address entries on the device. The administrator can check information about user access based on these MAC address entries to locate user access faults.

Precautions

If there are a lot of authen MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all authen MAC address entries in the system.

```
<HUAWEI> display mac-address authen
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                  Learned-From       Type
--------------------------------------------------------------------------------
xxxx-xxxx-xxxx 3000/-/-                     GE0/0/1            authen
xxxx-xxxx-xxx1 3000/-/-                     GE0/0/1            authen
xxxx-xxxx-xxx2 3000/-/-                     GE0/0/1            authen
--------------------------------------------------------------------------------
Total items displayed = 3
```

Table 13-104 Description of the **display mac-address authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/VSI/BD	VLAN/VSI/BD that the outbound interface belongs to.

Item	Description
Learned-From	Interface on which a MAC address is learned.
Type	Type of MAC addresses.
Total items displayed	Total number of MAC address entries that match the filter condition.

13.6.45 display mac-address pre-authen

Function

The **display mac-address pre-authen** command displays the current pre-authen MAC address entries in the system.

Format

display mac-address pre-authen [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check the existing MAC address entries of the pre-connection type to obtain access information about pre-connection users and locate faults.

Precautions

If there are a lot of pre-authen MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all pre-authen MAC address entries in the system.

```
<HUAWEI> display mac-address pre-authen
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                  Learned-From       Type
--------------------------------------------------------------------------------
00e0-fc00-0100 3000/-/-                     GE0/0/1            pre-authen
00e0-fc00-0400 3000/-/-                     GE0/0/1            pre-authen
00e0-fc00-0200 3000/-/-                     GE0/0/1            pre-authen
--------------------------------------------------------------------------------
Total items displayed = 3
```

Table 13-105 Description of the **display mac-address pre-authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/VSI/BD	VLAN/VSI/BD that the outbound interface belongs to.
Learned-From	Interface on which a MAC address is learned.
Type	Type of a MAC address entry.
Total items displayed	Total number of MAC address entries that match the filter condition.

13.6.46 display mac-authen

Function

The **display mac-authen** command displays information about MAC address authentication.

Format

display mac-authen [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> | **configuration**]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays information about MAC address authentication on a specified interface. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. MAC address authentication information on all device interfaces is displayed if this parameter is not specified.	-
configuration	Displays the global information about MAC address authentication.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display mac-authen** command to view configuration results of all configuration commands in MAC address authentication. The command output helps you to check whether the MAC address authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

You can locate the fault according to the packet statistics that is displayed using the **display mac-authen** command. When the fault is rectified, run the **reset mac-authen statistics** command to clear the packet statistics. After a period of time, run the **display mac-authen** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

View all information about MAC address authentication.

```
<HUAWEI> display mac-authen
  MAC address authentication is Enabled.
  Username format: use MAC address without-hyphen as username
  Quiet period is 60s
  Authentication fail times before quiet is 1
  Offline detect period is 300s
  Reauthenticate period is 1000s
  Guest user reauthenticate period is 60s
  Maximum users: 100
  Current users: 1
  Global domain is not configured
  Trigger condition: dhcp arp dhcpv6 nd

 GigabitEthernet0/0/1 state : UP. MAC address authentication is enabled
  Reauthentication is enabled
  Reauthen Period: 1000s
  Maximum users: 100
  Current users: 1
  Authentication Success: 0, Failure: 0

 Online user(s) info:
 UserId   MAC/VLAN          AccessTime            UserName
 ------------------------------------------------------------------------------
 16016    00e0-fc12-3456/2003 2014/01/26 09:22:49     wlan
 ------------------------------------------------------------------------------
 Total 1,1 printed
```

Table 13-106 Description of the **display mac-authen** command output

Item	Description
Mac address authentication is Enabled	MAC address authentication is enabled. To enable MAC address authentication, run the **mac-authen** command.

Item	Description
Username format	User name format for MAC address authentication. ● use MAC address without-hyphen as username: A user name is a MAC address that does not contain hyphens (-), for example, 00e0fc123456. ● use MAC address with-hyphen as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 00e0-fc12-3456. ● use MAC address with-hyphen normal as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-e0-fc-12-34-56. ● use MAC address without-hyphen upper as username: A user name is a MAC address in the uppercase format that does not contain hyphens (-), for example, 00E0FC123456. ● use MAC address with-hyphen upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 00E0-FC12-3456. ● use MAC address with-hyphen normal upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-E0-FC12-34-56. ● use MAC address with-hyphen colon as username: A user name is a MAC address that contains colons (:) and the colons are inserted between every four digits, for example, 00e0:fc12:3456. ● use MAC address with-hyphen normal colon as username: A user name is a MAC address that

Item	Description
	contains colons (:) and the colons are inserted between every two digits, for example, 00:e0:fc12:34:56. ● use MAC address with-hyphen colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every four digits, for example, 00E0:FC12:3456. ● use MAC address with-hyphen normal colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every two digits, for example, 00:E0:FC12:34:56. ● fixed username: The user name is fixed. ● use option82 as username: The content of the Option 82 field is used as the user name. ● not configured: The user name format is not configured. To configure a user name, run the **mac-authen username** command.
Quiet period	Quiet timer value, during which the user waits for re-authentication after the maximum number of authentication failures is exceeded. The default value of the quiet timer is 60 seconds. To set the quiet period, run the **mac-authen timer** command.
Authentication fail times before quiet	Maximum number of authentication failures before a MAC address authentication user enters the quiet state.
Offline detect period	Interval for detecting online users. The timer is used to periodically check whether a user is offline. The default interval is 300 seconds. To set the interval for detecting online users, run the **mac-authen timer** command.

Item	Description
Reauthenticate period is 1000s	Interval at which users are re-authenticated. The default interval is 1800 seconds. To set the re-authentication period, run the **mac-authen timer** command.
Guest user reauthenticate period is 60s	Interval at which users in a guest VLAN are re-authenticated. The default interval is 60 seconds. To set the guest VLAN user re-authentication period, run the **mac-authen timer** command.
Maximum users	Maximum number of online users allowed by the device, the value varies according to devices. To set the maximum number of MAC address authentication users on an interface, run the **mac-authen max-user** command.
Current users	Number of current online users.
Global domain	Current authentication domain. By default, no authentication domain is specified for users. If you do not specify any domain for users, the default domain in the system is used. To configure an authentication domain, run the **mac-authen domain** command.
Trigger condition	Packet type that can trigger MAC address authentication. To configure the packet type, run the **mac-authen trigger** command.
GigabitEthernet0/0/1 current state	Interface state. ● UP: The interface is started. ● DOWN: The interface is shut down.
MAC address authentication is Enabled	MAC address authentication is enabled on the interface. To enable MAC address authentication, run the **mac-authen** command.
Reauthentication is enabled	MAC address reauthentication is enabled. To enable the MAC address reauthentication, run the **mac-authen reauthenticate** command.

Item	Description
Reauthen Period	Interval at which users are re-authenticated. The default interval is 1800 seconds. To set the re-authentication period, run the **mac-authen timer reauthenticate-period** command.
Maximum users	Maximum number of MAC address authentication users on the interface. To set the maximum number of MAC address authentication users on an interface, run the **mac-authen max-user** command.
Current users	Number of current online users on the interface.
Authentication Success: 0, Failure: 0	Numbers of successful and failed authentications on the interface.
UserId	ID of an online user.
MAC/VLAN	MAC address and VLAN of a user. **NOTE** If the AAA server delivers an authorized VLAN, information about the authorized VLAN is displayed.
AccessTime	Access time of a user.
UserName	Name of a user.

13.6.47 display mac-authen quiet-user

Function

The **display mac-authen quiet-user** command displays information about MAC address authentication users who are quieted.

Format

display mac-authen quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all MAC address authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a specified MAC address authentication user who is quieted.	The value is in the H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about MAC address authentication users who are quieted.

Example

Display information about all MAC address authentication users who are quieted.

```
<HUAWEI> display mac-authen quiet-user all
--------------------------------------------------------------------------------
MacAddress              User status                 Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
00e0-fc02-0003          Block                       50
--------------------------------------------------------------------------------
Total: 1  Printed: 1  Block: 1  Active: 0
```

Table 13-107 Description of the **display mac-authen quiet-user all** command output

Item	Description
MacAddress	MAC address of a MAC address authentication user who is quieted.
User status	User status: • Block: The user is in a silent state. • Active: The user is not in a silent state.

Item	Description
Quiet Remain Time(Sec)	• If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. • If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.

13.6.48 display port connection-type access all

Function

The **display port connection-type access all** command displays all current downlink interfaces on the device.

Format

display port connection-type access all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check all current downlink interfaces on the device.

Example

Display all current downlink interfaces on the device.

```
<HUAWEI> display port connection-type access all
Slot 0:
GigabitEthernet0/0/1     GigabitEthernet0/0/2     GigabitEthernet0/0/3
GigabitEthernet0/0/4     GigabitEthernet0/0/5     GigabitEthernet0/0/6
GigabitEthernet0/0/7     GigabitEthernet0/0/8     GigabitEthernet0/0/9
GigabitEthernet0/0/10    GigabitEthernet0/0/11    GigabitEthernet0/0/12
GigabitEthernet0/0/13    GigabitEthernet0/0/14    GigabitEthernet0/0/15
GigabitEthernet0/0/16    GigabitEthernet0/0/17    GigabitEthernet0/0/18
GigabitEthernet0/0/19    GigabitEthernet0/0/20    GigabitEthernet0/0/21
GigabitEthernet0/0/22    GigabitEthernet0/0/23    GigabitEthernet0/0/24
```


Table 13-108 Description of the display port connection-type access all command output

Item	Description
Slot 0	Slot ID.
GigabitEthernet0/0/1	Interface name.

13.6.49 display portal

Function

The **display portal** command displays the Portal authentication configuration.

Format

display portal [**interface** *interface-type interface-number* | **configuration**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays Portal authentication configuration on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. Portal authentication configuration in the system view or on all interfaces is displayed if this parameter is not specified.	-
configuration	Displays the global Portal authentication configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display portal** command to view the Portal authentication configuration and check whether the configuration is correct.

Example

Display the Portal authentication configuration.

```
<HUAWEI> display portal
 Portal timer offline-detect length:500
 Portal max-user number:100
 Quiet function is Disabled
 Different-server is Disabled
 Parameter set: Quiet Period      60s   Quiet-times         3
 Logout packets resend: Resend-times 3  Timeout 5s
 Portal user(s) on slot 0:1

 Vlanif10 protocol status: up, web-auth-server layer2(direct)
   Portal domain: tsm
   Auth-network:
      10.3.3.3          255.255.255.255
      10.8.0.0          255.255.0.0
```

Display the Portal authentication configuration on VLANIF10.

```
<HUAWEI> display portal interface vlanif 10

 Vlanif10 protocol status: up, web-auth-server layer2(direct)
    Portal domain: tsm
    Auth-network:
      10.3.3.3          255.255.255.255
      10.8.0.0          255.255.0.0
```

Table 13-109 Description of the **display portal** command output

Item	Description
Portal timer offline-detect length	Portal authentication user offline detection interval. To set the user offline detection interval, run the **portal timer offline-detect** command.
Portal max-user number	Maximum number of concurrent Portal authentication users allowed to access the device, the value varies according to device models. To set the maximum number of concurrent Portal authentication users allowed to access the device, run the **portal max-user** command.
Quiet function is Enabled or Quiet function is Disabled	Whether the quiet function in Portal authentication is enabled. • Enabled • Disabled To enable the quiet function, run the **portal quiet-period** command.

Item	Description
Different-server is Enabled or Different-server is Disabled	Whether a device is enabled to process user logout requests sent by a Portal server other than the one from which users log in: ● Enabled ● Disabled To configure a device to process user logout requests sent by a Portal server other than the one from which users log in, command, run the **portal logout different-server enable** command.
Parameter set	Parameter settings of the quiet function in Portal authentication. ● Quiet Period: indicates the quiet period in Portal authentication. To set the quiet period in Portal authentication, run the **portal timer quiet-period** command. ● Quiet-times: indicates the maximum number of authentication failures within 60 seconds before a Portal authentication user enters the quiet state. To set the maximum number of authentication failures, run the **portal quiet-times** command.
Logout packets resend	Configuration of the logout packet re-transmission function for Portal authentication users. ● Resend-times: indicates the number of re-transmission times for Portal authentication user logout packets. ● Timeout: indicates the re-transmission interval of Portal authentication user logout packets. To set the re-transmission interval, run the **portal logout resend timeout** command.

Item	Description
Portal user(s) on slot 0	Statistics on Portal authentication users on the device. **NOTE** This parameter is unavailable when no Portal authentication user is online. When Portal authentication users go online through an Eth-Trunk, the number of Portal authentication users on the device where Eth-Trunk member interfaces are located is the same as the actual number of Portal authentication users on the device.
Vlanif10 protocol status	Link layer protocol state of the VLANIF interface. • up: indicates that the interface is running properly. • down: indicates that the interface is disabled. • web-auth-server layer2(direct): indicates that the authentication mode is set to Layer 2 Portal authentication on a specified interface.
Portal domain	Name of a forcible Portal authentication domain. To set a forcible Portal authentication domain, run the **portal domain** command.
Auth-network	Portal authentication subnet. To set the Portal authentication subnet, run the **portal auth-network** command.

13.6.50 display portal free-rule

Function

The **display portal free-rule** command displays authentication-free rules for Portal authentication users.

Format

display portal free-rule [*rule-id*]

Parameters

Parameter	Description	Value
rule-id	Displays the ID of an authentication-free rule. If the rule ID is not specified, the configuration of all authentication-free rules is displayed.	The value is an integer of which the range depends on product models.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display portal free-rule** command shows the configuration of authentication-free rules. You can locate faults according to the command output.

Example

Display the configuration of authentication-free rules.

```
<HUAWEI> display portal free-rule
portal free-rule 0 destination ip 10.1.1.1 mask 255.255.255.255
portal free-rule 10 destination ip 10.1.1.2 mask 255.255.255.255
Total 2 free-rules
```

Display the configuration of authentication-free rule 10.

```
<HUAWEI> display portal free-rule 10
portal free-rule 10 destination ip 10.1.1.1 mask 255.255.255.255
```

13.6.51 display portal https-redirect blacklist

Function

The **display portal https-redirect blacklist** command displays IPv4 addresses in the HTTPS redirection blacklist.

The **display portal https-redirect ipv6 blacklist** command displays IPv6 addresses in the HTTPS redirection blacklist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display portal https-redirect blacklist

display portal https-redirect ipv6 blacklist

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the addresses in the HTTPS redirection blacklist are correct.

Example

Display IPv4 addresses in the HTTPS redirection blacklist.

```
<HUAWEI> display portal https-redirect blacklist
---------------------------------------
IP Address        Aging Time
---------------------------------------
 10.1.1.1         2018-06-26 21:01:59
---------------------------------------
 Total:1    Print:1
```

Display IPv6 addresses in the HTTPS redirection blacklist.

```
<HUAWEI> display portal https-redirect ipv6 blacklist
-------------------------------------------------------------
IPv6 Address                          Aging Time
-------------------------------------------------------------
FC00::1                               2019-02-23 09:47:05
-------------------------------------------------------------
 Total:1    Print:1
```

Table 13-110 Description of the **display portal https-redirect blacklist** command output

Item	Description
IP Address/IPv6 Address	IPv4/IPv6 addresses in the blacklist, which is configured using the **portal https-redirect blacklist** command or is added after the condition specified by the **portal https-redirect blacklist packet-rate** or **portal https-redirect blacklist retry-times interval** command is met.

Item	Description
Aging Time	Time when an address in the blacklist is aged out (that is, time when an address is removed from the blacklist). You can run the **portal https-redirect blacklist aging-time** command to configure the aging time of addresses in the blacklist.
Total:*m* Print:*n*	Total number of addresses in the blacklist, and number of addresses displayed.

13.6.52 display portal https-redirect whitelist

Function

The **display portal https-redirect whitelist** command displays IPv4 addresses in the HTTPS redirection whitelist.

The **display portal https-redirect ipv6 whitelist** command displays IPv6 addresses in the HTTPS redirection whitelist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display portal https-redirect whitelist

display portal https-redirect ipv6 whitelist

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the addresses in the HTTPS redirection whitelist are correct.

Example

Display IPv4 addresses in the HTTPS redirection whitelist.

```
<HUAWEI> display portal https-redirect whitelist
IP Address:
--------------------------------
 10.1.2.1
--------------------------------
 Total:1    Print:1
```

Display IPv6 addresses in the HTTPS redirection whitelist.

```
<HUAWEI> display portal https-redirect ipv6 whitelist
IPv6 Address:
------------------------------------------------------------------
FC00::2
------------------------------------------------------------------
 Total:1    Print:1
```

Table 13-111 Description of the **display portal https-redirect whitelist** command output

Item	Description
IP Address/IPv6 Address	IPv4/IPv6 addresses in the whitelist, which are configured using the **portal https-redirect whitelist** command.
Total:*m* Print:*n*	Total number of addresses in the whitelist, and number of addresses displayed.

13.6.53 display portal quiet-user

Function

The **display portal quiet-user** command displays information about Portal authentication users in quiet state.

Format

display portal quiet-user { **all** | **server-ip** *ip-address* | **user-ip** { *ip-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Displays information about all Portal authentication users in quiet state.	-

Parameter	Description	Value
user-ip *ip-address*	Displays information about the quiet user with the specified IP address.	The value is in dotted decimal notation.
user-ip *ipv6-address*	Displays information about the quiet user with the specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
server-ip *ip-address*	Displays information about all the users in quiet state authenticated by the Portal authentication server with a specified IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the quiet timer is enabled, you can run the **display portal quiet-user** command to view information about Portal authentication users in quiet state.

Example

Display information about all Portal authentication users in quiet state.

```
<HUAWEI> display portal quiet-user all
Quiet IP information
--------------------------------------------------------------------------------
Quiet ip              User status             Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
192.168.1.1             Active                10
192.168.1.2             Block                 20
--------------------------------------------------------------------------------
Total: 2  Printed: 2  Block: 1   Active: 1
```

Display information about the user in quiet state at 192.168.1.1.

```
<HUAWEI> display portal quiet-user user-ip 192.168.1.1
  Quiet remain seconds: 50
  User Status: Active
```

Table 13-112 Description of the **display portal quiet-user** command output

Item	Description
Quiet IP information	Information about the user in quiet state.

Item	Description
Quiet ip	IP address of the user in quiet state.
User status	User status: • Block: The user is in silent state. • Active: The user is not in silent state. Currently, only users in silent state can be displayed.
Quiet Remain Time(Sec)	• If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. • If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.
Quiet remain seconds	Remaining quiet period of the user in quiet state, in seconds.

13.6.54 display portal user-logout

Function

The **display portal user-logout** command displays temporary logout entries of Portal authentication users.

Format

display portal user-logout [**ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Displays temporary logout entries of the Portal authentication user with a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays temporary logout entries of the Portal authentication user with a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device records temporary entries after Portal authentication users are disconnected. The network administrator can run this command to check temporary logout entries to locate faults.

If the parameter **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] is not specified, the temporary logout entries of all Portal authentication users are displayed.

Example

Display the temporary logout entries of all Portal authentication users.

```
<HUAWEI> display portal user-logout
-------------------------------------------------------------
UserIP          Vrf      Resend Times TableID
-------------------------------------------------------------
192.168.111.100 1        3            0
-------------------------------------------------------------
Total: 1, printed: 1
```

Table 13-113 Description of the **display portal user-logout** command output

Item	Description
UserIP	IP address of the Portal authentication user.
Vrf	VPN instance that the Portal authentication user belongs to.
Resend Times	Number of logout packet re-transmission times. To set the number of logout packet re-transmission times, run the **portal logout resend timeout** command.
TableID	Index of the temporary logout entry.
Total: *m*, printed: *n*	Total number of temporary logout entries and number of displayed entries.

13.6.55 display portal url-encode configuration

Function

The **display portal url-encode configuration** command displays the configuration of URL encoding and decoding.

Format

display portal url-encode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring URL encoding and decoding, you can run the **display portal url-encode configuration** command to check the configuration.

Example

Display the configuration of URL encoding and decoding.

```
<HUAWEI> display portal url-encode configuration
  Portal URL Encode : Disable
```

Table 13-114 Description of the **display portal url-encode configuration** command output

Item	Description
Portal URL Encode	Whether URL encoding and decoding are enabled: • Disable • Enable To configure the function, run the **portal url-encode enable** command.

13.6.56 display server-detect state

Function

The **display server-detect state** command displays the status of a Portal server.

Format

display server-detect state [**web-auth-server** *server-name*]

Parameters

Parameter	Description	Value
web-auth-server *server-name*	Displays information about the Portal server status configured in the specified Portal server template. If this parameter is not specified, status of all Portal servers is displayed.	The Portal server template name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

ou can run the **display server-detect state** command to check information about the Portal server status.

Example

Display information about the Portal server status configured in the Portal server template **abc**.

```
<HUAWEI> display server-detect state web-auth-server abc
  Web-auth-server     :    abc
  Total-servers       :    4
  Live-servers        :    1
  Critical-num        :    0
  Status              :    Normal
  Ip-address              Status
  192.168.2.1             UP
  192.168.2.2             DOWN
  192.168.2.3             DOWN
  192.168.2.4             DOWN
```


Table 13-115 Description of the **display server-detect state** command output

Item	Description
Web-auth-server	Name of the Portal server template.
Total-servers	Number of Portal servers configured.
Live-servers	Number of Portal servers in Up state.
Critical-num	Minimum number of Portal servers in Up state. If the number of Portal servers is less than this value, enable the survival function in the corresponding Portal server template view.
Status	Status of the Portal server. The values are as follows: ● Normal: normal state ● Abnormal: indicates that the Portal server is in abnormal state ● Permit-all: survival state
Ip-address	IP address of the Portal server.
Status	Whether the Portal server with the specified IP address is reachable. The values are as follows: ● UP: reachable ● DOWN: unreachable

13.6.57 display static-user

Function

The **display static-user** command displays static user information.

Format

display static-user [**domain-name** *domain-name* | **interface** *interface-type interface-number* | **ip-address** *start-ip-address* [*end-ip-address*] | **vpn-instance** *vpn-instance-name*] * [**detail**]

Parameters

Parameter	Description	Value
domain-name *domain-name*	Displays static user information in a specified domain.	The value is a string of 1 to 64 case-sensitive characters without spaces, asterisk (*), question mark (?), and double quotation marks ("). The value cannot be - or --.
interface *interface-type interface-number*	Displays static user information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ip-address *start-ip-address* [*end-ip-address*]	Displays static user information in a specified IP address range.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays static user information in a specified VPN instance.	The value must be an existing VPN instance name.
detail	Displays detailed information about static users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a static user is configured, you can run the **display static-user** command to view the static user information.

Example

Display information about all static users configured.


```
<HUAWEI> display static-user
 Not-update-ip enable status: No
 IP-address       Interface       MAC-address    VPN
--------------------------------------------------------------------------------
 10.1.1.1         GE0/0/3         -              -
 10.1.1.2         GE0/0/3         -              -
 10.1.1.3         GE0/0/3         -              -
 10.1.1.5         GE0/0/5         00e0-fc12-3456 -
 10.1.1.6         GE0/0/5         00e0-fc12-3456 -
 10.1.1.7         GE0/0/5         00e0-fc12-3456 -
 10.1.1.8         GE0/0/5         00e0-fc12-3456 -
 10.1.1.10        -               00e0-fc12-3478 -
 10.1.1.11        -               00e0-fc12-3478 -
 10.1.1.12        -               00e0-fc12-3478 -
--------------------------------------------------------------------------------
Total item(s) displayed = 10
```

Display detailed information about all static users.

```
<HUAWEI> display static-user detail
 Not-update-ip enable status: No
--------------------------------------------------------------------------------
  IP address                    : 10.1.1.2
  IP static user                : Yes
  Vpn-instance                  : -
  Domain-name                   : local
  Interface                     : -
  MAC address                   : -
  VLAN                          : 10
  Detect                        : Disable
  Keep-online                   : Disable
--------------------------------------------------------------------------------
  IP address                    : 10.1.1.4
  IP static user                : Yes
  Vpn-instance                  : -
  Domain-name                   : -
  Interface                     : -
  MAC address                   : -
  VLAN                          : 10
  Detect                        : Disable
  Keep-online                   : Enable
--------------------------------------------------------------------------------
Total item(s) number= 2, displayed number= 2

Ip-static-user enable status:
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Total item(s) number= 0, displayed number= 0
```

Table 13-116 Description of the **display static-user** command output

Item	Description
Not-update-ip enable status	Whether the device is disabled from updating IP addresses of static users: ● Yes ● No
IP-address/IP address	IP address of a static user.
Interface	Interface connected to a static user.
MAC-address/MAC address	MAC address of a static user.

Item	Description
VPN/Vpn-instance	VPN instance to which a static user belongs.
Total item(s) number= *m*, displayed number= *n*	The total number of entries is *m* and the number of displayed entries is *n*.
Ip-static-user enable status	Whether the function of identifying static users through IP addresses is enabled.
IP static user	Whether the user is a static user: ● Yes ● No
Domain-name	Domain to which a static user belongs.
VLAN	VLAN to which a static user belongs.
Detect	Whether the device is enabled to send ARP packets to trigger MAC address authentication for offline static users: ● Enable ● Disable
Keep-online	Whether a static user is kept online, with offline detection not performed. ● Enable ● Disable

13.6.58 display url-template

Function

The **display url-template** command displays information about URL templates.

Format

display url-template { **all** | **name** *template-name* }

Parameters

Parameter	Description	Value
all	Displays information about all configured URL templates.	-

Parameter	Description	Value
name *template-name*	Displays information about the URL template with a specified name.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a URL template is configured, run the **display url-template** command to view information about the URL template.

Example

Display information about all configured URL templates.

```
<HUAWEI> display url-template all
-------------------------------------------------------------------------------
 Index    Name                        URL     Start  Assignment  Isolate
                                    Number  Mark   Mark        Mark
-------------------------------------------------------------------------------
 0        test                         0      ?      =           &
 1        test2                        0      ?      =           &
-------------------------------------------------------------------------------
 Total 2
```

Display information about the URL template **test**.

```
<HUAWEI> display url-template name test
 Name : test
 URL  :
  1. http://10.1.1.1
 Start mark      : !
 Assignment mark : j
 Isolate mark    : =
 User MAC        :
 Redirect URL    :
 User IP address :
 Sysname         :
 Delimiter       : %
 Format          : normal    Login URL Key   : logiurl   Login URL      : http:\\example.com
```


Table 13-117 Description of the **display url-template** command output

Item	Description
Index	Index of a URL template.
Name	Name of a URL template.
URL	URL of the Portal server. For details, see **url**.
Start mark	Start character in the URL address. For details, see **parameter**.
Assignment mark	Assignment character in the URL address. For details, see **parameter**.
Isolate mark	Delimiter between URL addresses. For details, see **parameter**.
User MAC	MAC address of a user. For details, see **url-parameter**.
Redirect URL	URL in the original user packet. For details, see **url-parameter**.
User IP address	User IP address. For details, see **url-parameter**.
Sysname	Device name. For details, see **url-parameter**.
Delimiter	Delimiter between MAC addresses in URL. For details, see **url-parameter mac-address format**.
Format	Format MAC addresses in URL. For details, see **url-parameter mac-address format**.
Login URL Key	Identification keyword for the login URL sent to the Portal server during redirection. For details, see **url-parameter**.
Login URL	Device login URL. For details, see **url-parameter**.

13.6.59 display user-group

Function

The **display user-group** command displays the configuration of a user group.

Format

display user-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the configuration of a specified user group. The configurations of all user groups are displayed if this parameter is not specified.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display user-group** command to obtain the user group configuration and locate faults according to the command output.

Example

Display the configuration of all user groups.

```
<HUAWEI> display user-group
--------------------------------------------------------------------------------
ID   Group name                  Rule-num   User-num  Status
--------------------------------------------------------------------------------
0    abc                        0          0         disabled
--------------------------------------------------------------------------------
Total 1
```

NOTE

When the length of **Group name** exceeds 14 characters, the name is displayed in abridged mode.

Display the configuration about the user group **abc**.

```
<HUAWEI> display user-group abc
  User group ID          : 0   Group name             : abc   ACL ID               :   ACL rule number       : 0
User-num               : 0   VLAN                 :   Remark dscp          :   Remark 8021p          :
Status                 : disabled
```


Table 13-118 Description of the **display user-group** command output

Item	Description
ID	ID of the user group.
Rule-num	Number of ACL rules.
User group ID	ID of the user group.
Group name	Name of the user group.
ACL ID	ID of the ACL bound to the user group. To set the ACL ID, run the **acl-id** command.
ACL rule number	Number of ACL rules.
User-num	Number of online users bound to the user group.
VLAN	VLAN of the user group. To set the VLAN, run the **user-vlan** command.
Remark dscp	Priorities for processing IP packets. To set the priorities, run the **remark** command.
Remark 8021p	Priorities for processing Ethernet Layer 2 packets. To set the priorities, run the **remark** command.
Status	Status of the user group. • disabled: The user group is disabled. • enabled: The user group is enabled.

13.6.60 display web-auth-server configuration

Function

The **display web-auth-server configuration** command displays the Portal server configuration.

Format

display web-auth-server configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the Portal server template is configured, the **display web-auth-server configuration** displays the Portal server configuration.

Example

Display the Portal server configuration.

```
<HUAWEI> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled
 ------------------------------------------------------------------------------
   Enabled protocol      : https
   Listening port        : 8443
   SSL policy            : default_policy
------------------------------------------------------------------------------
  Web-auth-server Name : test
  Web-auth-server Index: 0
  IP-address           :
  IPv6 Address         :
  Shared-key           :
  Source-IP            : -
  Port / PortFlag      : 50100 / NO
  URL                  : https://192.168.2.10:8443/webauth
  URL Template         :
  URL Template ParaName:
  URL Template IVName  :
  URL Template Key     :
  Redirection          : Enable
  Sync                 : Disable
  Sync Seconds         : 300
  Sync Max-times       : 3
  Detect               : Disable
  Detect Seconds       : 60
  Detect Max-times     : 3
  Detect Critical-num  : 0
  Detect Action        :
  Detect Type          : portal
  VPN Instance         :
  Bound Vlanif         :
  Bound Interface      :
  Protocol             : http
  Http Get-method      : disable
  Password Encrypt     : none
  Cmd ParseKey         : cmd
  Username ParseKey    : username
  Password ParseKey    : password
  MAC Address ParseKey : macaddress
  IP Address ParseKey  : ipaddress
  Initial URL ParseKey : initurl
  Login Cmd            : login
  Logout Cmd           : logout
  Login Success
      Reply Type       : redirect initial URL
      Redirect URL     :
```



```
    Message        : LoginSuccess!
Login Fail
    Reply Type     : redirect login URL
    Redirect URL   :
    Message        : LoginFail!
Logout Success
    Reply Type     : message
    Redirect URL   :
    Message        : LogoutSuccess!
Logout Fail
    Reply Type     : message
    Redirect URL   :
    Message        : LogoutFail!
------------------------------------------------------------------------------
1 Web authentication server(s) in total
```

Table 13-119 Description of the **display web-auth-server configuration** command output

Item	Description
Listening port	Listening port for Portal protocol packets. To configure a listening port, run the **web-auth-server listening-port** command.
Portal	Portal protocol version. ● version 1, version 2: The device supports both the versions V1.0 and V2.0. ● version 2: The device supports the versions V2.0. To configure the Portal protocol version, run the **web-auth-server version** command.
Include reply message	Whether the packets sent from the device to the Portal server contain authentication responses. ● enabled ● disabled To enable the device to transparently transmit authentication responses of users sent by the authentication server to the Portal server, run the **web-auth-server reply-message** command.
Enabled protocol	Enabled HTTP or HTTPS protocol. ● http ● https To enable the HTTP or HTTPS protocol, run the **portal web-authen-server** command.

Item	Description
Listening port	HTTP or HTTPS port number. To configure the HTTP or HTTPS port number, run the **portal web-authen-server** command.
SSL policy	SSL policy referenced by the HTTPS protocol. To configure the SSL policy referenced by the HTTPS protocol, run the **portal web-authen-server** command.
Web-auth-server Name	Name of the Portal server template. To configure the Portal server template name, run the **web-auth-server** command.
Web-auth-server Index	Index of the Portal server template.
IP-address	IPv4 address of the Portal server. To configure the IP address of the Portal server, run the **server-ip** command.
IPv6 Address	IPv6 address of the Portal server. To configure the IP address of the Portal server, run the **server-ip** command.
Shared-key	Shared key of the Portal server. To configure the shared key of the Portal server, run the **shared-key** command.
Source-IP	IP address used for communication with the Portal server. To configure the IP address used for communication with the Portal server, run the **source-ip** command.
Port / PortFlag	• Port: indicates the port number of the Portal server. • PortFlag: indicates whether packets are always sent through this port. To configure the port number of the Portal server, run the **port** command.
URL	URL of the Portal server. To configure the URL of the Portal server, run the **url** command.

Item	Description
URL Template	URL template bound to the Portal server template. To configure the URL template, run the **url-template** command.
Redirection	Redirection status of Portal authentication. ● Disable: Redirection of Portal authentication is disabled. ● Enable: Redirection of Portal authentication is enabled. To configure redirection of Portal authentication, run the **web-redirection disable** command.
Sync	User information synchronization. ● Disable ● Enable To enable user information synchronization, run the **user-sync** command.
Sync Seconds	User information synchronization interval. To set the user information synchronization interval, run the **user-sync** command.
Sync max-times	Maximum number of times that user information synchronization fails. To set the maximum number of times that user information synchronization fails, run the **user-sync** command.
Detect	Portal server detection and keepalive functions. ● Disable ● Enable To configure Portal server detection and keepalive functions, run the **server-detect** command.
Detect Seconds	Detection interval of the Portal server. To set the detection interval of the Portal server, run the **server-detect** command.
Detect max-times	Maximum number of detection failures. To set the maximum number of detection failures, run the **server-detect** command.

Item	Description
Detect Critical-num	Minimum number of Portal servers in Up state. If the number of running Portal servers is less than the minimum, enable the survival function in the corresponding Portal server template view. To configure this function, run the **server-detect** command.
Detect Action	Action taken after the number of detection failures exceeds the maximum. ● log: The device sends logs after the number of detection failures exceeds the maximum. ● trap: The device sends traps after the number of detection failures exceeds the maximum. ● permit-all: Portal authentication on the interface is disabled after the number of detection failures exceeds the maximum. To configure an action taken after the number of detection failures exceeds the maximum, run the **server-detect** command.
Detect Type	Portal server detection mode. ● Portal: Portal-based Portal server detection mode ● HTTP: HTTP-based Portal server detection mode
Bound Vlanif	VLANIF interface to which the Portal server template is bound. To bind the Portal server template to a VLANIF interface, run the **web-auth-server (Portal access profile view)**.
VPN instance	VPN instance used for Portal authentication. To configure a VPN instance, run the **vpn-instance** command.
Bound Interface	Ethernet interface or Eth-Trunk to which the Portal server template is bound. To bind the Portal server template to an Ethernet interface or Eth-Trunk, run the **web-auth-server (Portal access profile view)** command.

Item	Description
Http Get-method	Whether users submit user name and password information to the device in GET mode: • disable: GET mode is not used. • enable: GET mode is used. To configure the GET mode, run the **http get-method enable** command.
Protocol	Protocol used in Portal authentication. • portal • http To configure the protocol used in Portal authentication, run the **protocol** command.
Password Encrypt	Password encoding mode: • none: The password is not encoded. • uam: The password is encoded using ASCII character. To configure the password encoding mode, run the **protocol** command.
Cmd ParseKey	Command identification keyword. To configure the command identification keyword, run the **http-method post** command.
Username ParseKey	User name identification keyword. To configure the user name identification keyword, run the **http-method post** command.
Password ParseKey	User password identification keyword. To configure the user password identification keyword, run the **http-method post** command.
MAC Address ParseKey	User MAC address identification keyword. To configure the user MAC address identification keyword, run the **http-method post** command.
IP Address ParseKey	User IP address identification keyword. To configure the user IP address identification keyword, run the **http-method post** command.

Item	Description
Initial URL ParseKey	User initial login URL identification keyword. To configure the user initial login URL identification keyword, run the **http-method post** command.
Login Cmd	User login identification keyword. To configure the user login identification keyword, run the **http-method post** command.
Logout Cmd	User logout identification keyword. To configure the user logout identification keyword, run the **http-method post** command.
Login Success	User login success.
Reply Type	Redirection response type. ● redirect initial URL: A user is redirected to the initial login URL after successful login. ● redirect login URL: A user is redirected to the login URL after a login failure. ● message: specifies the displayed message. ● redirect URL: A user is redirected to a specified URL. To configure the redirection response type, run the **http-method post** command.
Redirect URL	Redirect URL. To configure the redirect URL, run the **http-method post** command.
Message	Displayed message. To configure the displayed message, run the **http-method post** command.
Login Fail	User login failure.
Logout Success	User logout success.
Logout Fail	User logout failure.

13.6.61 device-sensor dhcp option

Function

The **device-sensor dhcp option** command enables the DHCP-based terminal type awareness function.

The **undo device-sensor dhcp option** command disables the DHCP-based terminal type awareness function.

By default, the DHCP-based terminal type awareness function is disabled.

Format

device-sensor dhcp option *option-code* &<1-6>

undo device-sensor dhcp option *option-code* &<1-6>

Parameters

Parameter	Description	Value
option-code	Specifies the DHCP option field that the device needs to resolve. The option fields in a DHCP packet carry the control information and parameters, for example, terminal type.	The value is an integer that ranges from 1 to 254.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

After the DHCP-based terminal type awareness function is enabled, the device can resolve the option fields that carry terminal type information in the received DHCP Request packets. The device then sends the option information to the RADIUS server through RADIUS accounting packets. Through the option information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- To make this command take effect, you must run the **dhcp snooping enable** command on the interfaces or in VLANs.

Example

Set the option fields to be resolved by the device to option 60.

```
<HUAWEI> system-view
[HUAWEI] device-sensor dhcp option 60
```

13.6.62 device-sensor lldp tlv

Function

The **device-sensor lldp tlv** command enables the LLDP-based terminal type awareness function.

The **undo device-sensor lldp tlv** command disables the LLDP-based terminal type awareness function.

By default, the LLDP-based terminal type awareness function is disabled.

Format

device-sensor lldp tlv *tlv-type* &<1-4>

undo device-sensor lldp tlv

Parameters

Parameter	Description	Value
tlv-type	Specifies the LLDP TLV type as the terminal type to be aware of the device.	The value is an integer that can be 1, 2, 5, 6, 7, 8, and 127. The values are as follows: • 1: Chassis ID TLV, indicating the bridge MAC address of the device • 2: Port ID TLV, indicating the port identifying the LLD PDU sending end • 5: System Name TLV, indicating the device name • 6: System Description TLV, indicating the system description • 7: System Capabilities TLV, indicating the system capabilities • 8: Management Address TLV, indicating the management address • 127: Organization Specific TLV, indicating the user-defined organization information. You can run the **lldp tlv-enable med-tlv** command on the physical interface for user access to set this parameter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

Using the LLDP-based terminal type awareness function, the device parses the required TLV type containing terminal type information from the received LLDP packets. The device then sends the TLV type information to the RADIUS server through a RADIUS accounting packet. Through the TLV type information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- The command takes effect only when the LLDP function is enabled on the device and the connected peer device.

Example

Enable the terminal type awareness function based on LLDP TLV type 5.

```
<HUAWEI> system-view
[HUAWEI] device-sensor lldp tlv 5
```

13.6.63 dot1x authentication-method

Function

The **dot1x authentication-method** command sets the authentication mode for 802.1X users.

The **undo dot1x authentication-method** command restores the default authentication mode for 802.1X users.

By default, the global 802.1X user authentication mode is CHAP authentication and the 802.1X user authentication mode on interfaces is the same as the mode globally configured.

Format

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

Parameters

Parameter	Description	Value
chap	Indicates the CHAP-based EAP termination authentication mode.	-
pap	Indicates the PAP-based EAP termination authentication mode.	-
eap	Indicates that the EAP relay mode.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, users exchange authentication information with the device using EAP packets. The device uses two modes to exchange authentication information with the RADIUS server.

- EAP termination: The device directly parses EAP packets, encapsulates user authentication information into a RADIUS packet, and sends the RADIUS packet to the RADIUS server for authentication. In EAP termination authentication mode, the device and RADIUS server exchange information using PAP or CHAP.
  - PAP: The device arranges the MAC address, shared key, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the User-Password attribute.
  - CHAP: The device arranges the CHAP ID, MAC address, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the CHAP-Password and CHAP-Challenge attributes.

  After the device directly parses EAP packets, user information in the EAP packets is authenticated by a local AAA module, or sent to the RADIUS or HWTACACS server for authentication.
- EAP relay (specified by **eap**): The device encapsulates EAP packets into RADIUS packets and sends the RADIUS packets to the RADIUS server, but does not parse the received EAP packets that include user authentication information. This mechanism is called EAP over Radius (EAPOR).

The EAP relay mechanism requires that the RADIUS server be capable of parsing a lot of EAP packets and carrying out authentication; therefore, if the RADIUS server has high processing capabilities, the EAP relay is used. If the RADIUS server is incapable of parsing a lot of EAP packets and carrying out authentication, EAP termination is recommended, and the device helps the RADIUS server to parse EAP packets.

NOTE

- The authentication mode can be set to EAP relay for 802.1X authentication users only when the RADIUS authentication is used.
- If the 802.1X client uses the MD5 encryption mode, the user authentication mode on the device can be set to EAP or CHAP; if the 802.1X client uses the PEAP authentication mode, the authentication mode on the device can be set to EAP.

Example

Set the authentication mode to EAP for 802.1X users in the device in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x authentication-method eap
```

Set the authentication mode to EAP for 802.1X users on GE0/0/1.


```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x authentication-method eap
```

13.6.64 dot1x dhcp-trigger

Function

The **dot1x dhcp-trigger** command enables DHCP-triggered 802.1X authentication.

The **undo dot1x dhcp-trigger** command disables DHCP-triggered 802.1X authentication.

By default, DHCP-triggered 802.1X authentication is disabled.

Format

dot1x dhcp-trigger

undo dot1x dhcp-trigger

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP-triggered 802.1X authentication is enabled using the **dot1x dhcp-trigger** command, the device sends an 802.1X authentication-start packet to the user when receiving a DHCP Request message from the user. When the user receives the 802.1X authentication-start packet from the device, the 802.1X authentication page is displayed on the client device and prompts the user to enter the user name and password for authentication. During 802.1X network deployment, DHCP-triggered 802.1X authentication enables 802.1X users to start 802.1X authentication without dial-up using the client software, which facilitates network deployment.

NOTE

After receiving the request packet from an 802.1X user, the device starts authenticating the user. If the user is authenticated, the device allocates an IP address to the user through a DHCP server; if the user fails the authentication, the user cannot obtain a dynamic IP address from the DHCP server.

Prerequisites

802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.

Precautions

The **dot1x dhcp-trigger** command can be used only when the client supports DHCP and 802.1X authentication.

Example

Enable DHCP-triggered 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x dhcp-trigger
```

13.6.65 dot1x domain

Function

The **dot1x domain** command configures a forcible domain for 802.1X authentication users.

The **undo dot1x domain** command restores the default setting of a forcible domain for 802.1X authentication users.

By default, no forcible domain is configured for 802.1X authentication users.

Format

dot1x domain *domain-name*

undo dot1x domain

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a forcible domain.	The value must be an existing domain name on the device.

Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During authentication, if the user name entered by a user does not contain a domain name, the user will be authenticated in the default domain; if the user name contains a domain name, the user will be authenticated in the specified domain.

If the user names entered by many users do not contain domain names, excess users are authenticated in the default domain, making the authentication scheme inflexible. If all users on an interface need to use the same AAA scheme when the user names entered by some users contain domain name and those entered by other users do not, the device also cannot meet such requirement. To address this issue, you can configure a forcible domain. Then all users on the interface will be authenticated in the forcible domain no matter whether the user names entered by the users contain domain names.

Prerequisites

A domain has been created using the **domain** command.

Example

Configure the forcible domain **test** for 802.1X authentication users on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] quit
[HUAWEI-aaa] quit
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x domain test
```

13.6.66 dot1x eap-notify-packet

Function

The **dot1x eap-notify-packet** command enables the device to send an EAP packet code number to users.

The **undo dot1x eap-notify-packet** command disables the device from sending an EAP packet code number to users.

By default, the device is disabled from sending an EAP packet code number to users.

Format

dot1x eap-notify-packet eap-code *code-number* **data-type** *type-number*

undo dot1x eap-notify-packet [**eap-code** *code-number* **data-type** *type-number*]

Parameters

Parameter	Description	Value
eap-code *code-number*	Specifies an EAP packet code number sent to users.	The value is an integer that ranges from 5 to 255.
data-type *type-number*	Specifies the data type in EAP packets sent to users.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a non-Huawei device used as the RADIUS server sends RADIUS packets with attribute 61, EAP packet code number 0xa (hexadecimal notation, 10 in decimal notation), and data type 0x19 (hexadecimal notation, 25 in decimal notation) to the device, run the **dot1x eap-notify-packet** command on the device so that the device can send EAP packets with code number 0xa and data type 0x19 to users. If the **dot1x eap-notify-packet** command is not executed, the device does not process EAP packets of this type and users are disconnected.

Precautions

The device can only process EAP packets with code number 10 and data type 25.

Example

Allow the device to send EAP packets with code number 10 and data type 25 to users.

```
<HUAWEI> system-view
[HUAWEI] dot1x eap-notify-packet eap-code 10 data-type 25
```

13.6.67 dot1x enable

Function

The **dot1x enable** command enables 802.1X authentication on a device.

The **undo dot1x enable** command disables 802.1X authentication on a device.

By default, 802.1X authentication is disabled on a device.

Format

In the system view:

dot1x enable [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

undo dot1x enable [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

In the interface view:

dot1x enable

undo dot1x enable

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Enables 802.1X authentication on the specified interface of the device. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. Global 802.1X authentication is enabled if this parameter is not specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IEEE 802.1X standard (802.1X for short) is a port-based network access control protocol. You can run the **dot1x enable** command to enable 802.1X authentication globally and on an interface.

To make the 802.1X configuration effective on an interface, enable the global 802.1X authentication function and perform either of the following operations:

- Run the **dot1x enable** command in the interface view.
- Run the **dot1x enable interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> command in the system view.

Precautions

- All users have been disconnected before the **undo** operation is executed.
- After the static MAC address entry is configured using the **mac-address static** *mac-address interface-type interface-number* **vlan** *vlan-id* command, the user corresponding to the entry cannot pass 802.1X authentication.
- If 802.1X authentication is enabled on an interface, the following commands cannot be used on the same interface.

Command	Function
mac-limit	Sets the maximum number of MAC addresses that can be learned by an interface.
mac-address learning disable	Disables MAC address learning on an interface.
port link-type dot1q-tunnel	Sets the link type of an interface to QinQ.
port vlan-mapping vlan map-vlan **port vlan-mapping vlan inner-vlan**	Configures VLAN mapping on an interface.
port vlan-stacking	Configures selective QinQ.
mac-vlan enable	Enables MAC address-based VLAN assignment on an interface.
ip-subnet-vlan enable	Enables IP subnet-based VLAN assignment on an interface.

Command	Function
user-bind ip sticky-mac	Enables the device to generate snooping MAC entries.

Example

Enable 802.1X authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] dot1x enable interface gigabitethernet 0/0/1
```

Enable 802.1X authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x enable
```

13.6.68 dot1x free-ip

Function

The **dot1x free-ip** command configures a free IP subnet.

The **undo dot1x free-ip** command deletes the configured free IP subnet.

By default, no free IP subnet is configured.

Format

dot1x free-ip *ip-address* { *mask-length* | *mask-address* }

undo dot1x free-ip { *ip-address* { *mask-length* | *mask-address* } | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies a free IP subnet.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of an IP address.	The value is an integer that ranges from 1 to 32.
mask-address	Specifies the mask of the IP address.	The value is in dotted decimal notation.
all	Deletes all free IP subnets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

802.1X users can access networks only after being authenticated. You can configure a free IP subnet, so that users can access network resources in the free IP subnet before being authenticated.

Precautions

- 802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.
- To ensure that pre-connection users can be aged out normally, you need to run the **dot1x timer free-ip-timeout** command to set the aging time of authentication-free user entries.
- After the free-ip function is configured, the guest VLAN, critical VLAN, and restrict VLAN are no longer effective.
- The free IP subnet takes effect only when the interface authorization state is auto.
- If a user who does not pass 802.1X authentication wants to obtain an IP address dynamically through the DHCP server, the network segment of the DHCP server needs to be configured to a free IP subnet so that the user can access the DHCP server.
- After 802.1X users go offline, they are not allowed to access network resources on free IP subnets within a specified period to prevent malicious attacks.
- After users succeed in 802.1X-based fast deployment, they can only access resources in the IP free subnets and some resources on the device.

Example

Configure 192.168.1.0/24 as a free IP subnet that users can access before they pass 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x free-ip 192.168.1.0 24
```

13.6.69 dot1x mac-bypass

Function

The **dot1x mac-bypass** command enables MAC address bypass authentication on an interface.

The **undo dot1x mac-bypass** command disables MAC address bypass authentication on an interface.

By default, MAC address bypass authentication is disabled on an interface.

Format

In the system view:

dot1x mac-bypass { **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> }

undo dot1x mac-bypass { **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> }

In the interface view:

dot1x mac-bypass

undo dot1x mac-bypass

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Enables MAC address bypass authentication on the specified interface. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable MAC address bypass authentication for terminals (for example, printers) on which the 802.1X client software cannot be installed or used.

After MAC address bypass authentication is enabled on the interface using the **dot1x mac-bypass** command, the device first performs 802.1X authentication on users. If the user name request times out, the device starts the MAC address authentication process for the users. When 802.1X authentication fails, the device does not start the MAC address authentication process.

NOTE

Running the **dot1x mac-bypass** command also enables 802.1X authentication on an interface, and running the **undo dot1x mac-bypass** command also disables 802.1X authentication on an interface. When you run the **dot1x mac-bypass** command on an interface that has been enabled with 802.1X authentication, the authentication mode on the interface changes to MAC address bypass authentication.

Prerequisites

802.1X authentication has been enabled globally using the **dot1x enable** command.

Example

Enable MAC address bypass authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x mac-bypass interface gigabitethernet 0/0/1
```

Enable MAC address bypass authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x mac-bypass
```

13.6.70 dot1x mac-bypass access-port

Function

The **dot1x mac-bypass access-port** command enables MAC address bypass authentication on all downlink interfaces of the device.

The **undo dot1x mac-bypass access-port** command disables MAC address bypass authentication on all downlink interfaces of the device.

By default, MAC address bypass authentication is disabled on all downlink interfaces of the device.

Format

dot1x mac-bypass access-port all

undo dot1x mac-bypass access-port all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable MAC address bypass authentication for terminals (such as printers) on which the 802.1X client software cannot be installed or used.

After MAC address bypass authentication is enabled, the device performs 802.1X authentication on a user. Once 802.1X authentication fails, the device sends the user's MAC address as the user name and password to the authentication server.

NOTE

MAC address bypass authentication involves 802.1X authentication. That is, the **dot1x mac-bypass access-port all** command also enables 802.1X authentication on the interfaces; the **undo dot1x mac-bypass access-port all** command also disables 802.1X authentication on the interfaces. If 802.1X authentication has been enabled on the interfaces, the authentication mode on the interfaces is changed to MAC address bypass authentication after you run the **dot1x mac-bypass access-port all** command.

Prerequisites

802.1X authentication has been enabled globally and on the interfaces using the **dot1x enable** command.

Example

In the system view, enable MAC address bypass authentication on all downlink interfaces of the device.

```
<HUAWEI> system-view
[HUAWEI] dot1x mac-bypass access-port all
```

13.6.71 dot1x mac-bypass mac-auth-first

Function

The **dot1x mac-bypass mac-auth-first** command enables the device to perform MAC address authentication first during MAC address bypass authentication.

The **undo dot1x mac-bypass mac-auth-first** command disables the device from performing MAC address authentication first during MAC address bypass authentication.

By default, the MAC address authentication is not performed first during MAC address bypass authentication.

Format

In the system view:

dot1x mac-bypass mac-auth-first interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x mac-bypass mac-auth-first interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x mac-bypass mac-auth-first

undo dot1x mac-bypass mac-auth-first

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Enables the device to perform MAC address authentication first on a specified interface during MAC address bypass authentication. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both the clients that do not support 802.1X authentication (such as printers) and the clients that support 802.1X authentication (such as PCs) are connected to the interface enabled with MAC address bypass authentication, you can run the **dot1x mac-bypass mac-auth-first** command to enable the device to perform MAC address authentication first during MAC address bypass authentication. After that, the device first starts the MAC address authentication process for users, and triggers 802.1X authentication only if MAC address authentication fails.

Prerequisites

802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.

Follow-up Procedure

Run the **dot1x mac-bypass** command to enable MAC address bypass authentication on the interface.

Example

Enable the device to first perform MAC address authentication on GE0/0/1 during MAC address bypass authentication in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x mac-bypass mac-auth-first interface gigabitethernet 0/0/1
```

Enable the device to first perform MAC address authentication on GE0/0/1 during MAC address bypass authentication in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x mac-bypass mac-auth-first
```

13.6.72 dot1x max-user

Function

The **dot1x max-user** command sets the maximum number of 802.1X authentication users allowed on an interface.

The **undo dot1x max-user** command restores the default maximum number of 802.1X authentication users allowed on an interface.

By default, the number of 802.1X authentication users is the maximum number of 802.1X authentication users supported by the device.

Format

In the system view:

dot1x max-user *user-number* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x max-user [*user-number*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x max-user *user-number*

undo dot1x max-user [*user-number*]

Parameters

Parameter	Description	Value
user-number	Specifies the maximum number of 802.1X authentication users on an interface.	The value is an integer that varies depending on the product model.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To limit the maximum number of 802.1X authentication users allowed on an interface, run the **dot1x max-user** command.

Prerequisites

The 802.1X authentication function has been enabled globally and on an interface using the **dot1x enable** command.

Precautions

If the user access mode on an interface is interface-based (configured using the **dot1x port-method** command), the maximum number of 802.1X authentication users allowed on the interface is 1. Before running the **dot1x max-user** command to set the maximum number of 802.1X authentication users allowed on the interface, run the **undo dot1x port-method** command to restore the user access mode on the interface to MAC address-based.

Example

In the system view, set the maximum number of 802.1X authentication users allowed on GE0/0/1 to 7.

```
<HUAWEI> system-view
[HUAWEI] dot1x max-user 7 interface gigabitethernet 0/0/1
```

In the interface view, set the maximum number of 802.1X authentication users allowed on GE0/0/1 to 7.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x max-user 7
```

13.6.73 dot1x mc-trigger

Function

The **dot1x mc-trigger** enables multicast-triggered 802.1X authentication.

The **undo dot1x mc-trigger** disables multicast-triggered 802.1X authentication.

By default, multicast-triggered 802.1X authentication is enabled.

Format

dot1x mc-trigger

undo dot1x mc-trigger

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a client (for example, the built-in 802.1X client of the Windows operating system) cannot send an EAPOL-Start packet to perform 802.1X authentication, you can enable multicast-triggered 802.1X authentication. After that, the device multicasts an Identity EAP-Request frame to the client to trigger authentication.

Prerequisites

802.1X authentication has been enabled globally and on the interface using the **dot1x enable** command.

Example

Enable multicast-triggered 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x mc-trigger
```

13.6.74 dot1x mc-trigger port-up-send enable

Function

The **dot1x mc-trigger port-up-send enable** command enables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

The **undo dot1x mc-trigger port-up-send enable** command disables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

By default, the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is disabled.

Format

dot1x mc-trigger port-up-send enable

undo dot1x mc-trigger port-up-send enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device periodically multicasts EAP-Request/Identity packets to clients so that the clients are triggered to send EAPOL-Start packets for 802.1X authentication. If the device interface connecting to a client changes from Down to Up, the client needs to send EAPOL-Start packets again for 802.1X authentication, which takes a long time. You can run the **dot1x mc-trigger port-up-send enable** command on the device to enable the device interface to multicast EAP-Request/Identity packets to the client to trigger 802.1X authentication immediately after the interface goes Up. This configuration shortens the re-authentication time.

Precautions

When the access control mode on the device interface is based on the MAC address, the **dot1x mc-trigger port-up-send enable** command does not take effect.

Example

Enable the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

```
<HUAWEI> system-view
[HUAWEI] dot1x mc-trigger port-up-send enable
```

13.6.75 dot1x port-control

Function

The **dot1x port-control** command sets the authorization state of an interface.

The **undo dot1x port-control** command restores the default authorization state of an interface.

By default, the authorization state of an interface is **auto**.

Format

In the system view:

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** } **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x port-control interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** }

undo dot1x port-control

Parameters

Parameter	Description	Value
auto	Indicates the auto identification mode. In this mode, an interface is initially in Unauthorized state and only allows users to send and receive authentication packets. Users cannot access network resources. After the users are authenticated, the interface becomes authorized and allows the users to access network resources.	-
authorized-force	Indicates the forcible authorization mode. In this mode, the interface is always in Authorized state, does not handle authentication packets, and allows users to access network resources without authentication or authorization.	-

Parameter	Description	Value
unauthorized-force	Indicates the forcible unauthorized mode. In this mode, the interface is always in Unauthorized state, does not handle authentication packets, and prohibits users from accessing network resources.	-
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **auto** mode is recommended. Only authenticated users can access network resources. To trust all users on an interface without authentication, configure the **authorized-force** mode. To disable access rights of all users on an interface to ensure security, configure the **unauthorized-force** mode.

Prerequisites

802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.

Precautions

When there are online 802.1X users on an interface, the **dot1x port-control** command must not be run; otherwise, the system displays alarm information.

It is recommended that you set the authorization state of an interface in the early stage of network deployment. When the network is running properly, run the **cut access-user** command to disconnect all users from the interface before changing the authorization state.

Example

Set the authorization state of GE0/0/1 to **unauthorized-force** in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x port-control unauthorized-force interface gigabitethernet 0/0/1
```

Set the authorization state of GE0/0/1 to **unauthorized-force** in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x port-control unauthorized-force
```

13.6.76 dot1x port-method

Function

The **dot1x port-method** command sets the 802.1X access control method of an interface.

The **undo dot1x port-method** command sets the default 802.1X access control method of an interface.

By default, 802.1X access control on an interface is based on MAC addresses.

Format

In the system view:

dot1x port-method { **mac** | **port** } **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x port-method interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x port-method { **mac** | **port** }

undo dot1x port-method

Parameters

Parameter	Description	Value
mac	Indicates that users are authenticated based on their MAC addresses.	-
port	Indicates that users are authenticated based on their access interfaces.	-
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Indicates the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

802.1X access control can be based on MAC addresses or interfaces.

- When the **mac** method is used, all 802.1X users on an interface are authenticated one by one. If a user goes offline, other users on this interface are not affected. The **mac** method is applicable to individual users.
- When the **port** method is used, all the other 802.1X users on an interface can use network resources as long as one user is authenticated successfully. When the authenticated user goes offline, other users cannot use network resources. The **port** method is applicable to group users.

Prerequisites

802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.

Precautions

- When there are online 802.1X users on an interface, do not run the **dot1x port-method** command to change the access control method on the interface.
- If the access control method of an interface is set to **port**, only one 802.1X users can access the interface. After you run the **undo dot1x port-method** command, MAC address-based access control is enabled, but still only one user can access the interface. You can run the **dot1x max-user** command to increase the maximum number of 802.1X users as required.

Example

Set the 802.1X access control method on GE0/0/1 in the system view to **port**.

```
<HUAWEI> system-view
[HUAWEI] dot1x port-method port interface gigabitethernet 0/0/1
```

Set the 802.1X access control method on GE0/0/1 in the interface view to **port**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x port-method port
```

13.6.77 dot1x quiet-period

Function

The **dot1x quiet-period** command enables the quiet timer function.

The **undo dot1x quiet-period** command disables the quiet timer function.

By default, the quiet timer function is enabled.

Format

dot1x quiet-period

undo dot1x quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the quiet timer function is enabled, if the number of authentication failures of an 802.1X user exceeds a specified value (set using the **dot1x quiet-times** command) within 60 seconds, the user enters a quiet period. During the quiet period, the device discards the 802.1X authentication request packets from the user. This prevents the impact on the system due to frequent user authentication.

The value of the quiet timer is set using the **dot1x timer** command. When the quiet timer expires, the device re-authenticates the user.

Precautions

To make the configuration take effect, run the **dot1x enable** command twice to enable global and interface-based 802.1X user authentication.

Example

Enable the quiet timer.

```
<HUAWEI> system-view
[HUAWEI] dot1x quiet-period
```

13.6.78 dot1x quiet-times

Function

The **dot1x quiet-times** command sets the maximum number of authentication failures within 60 seconds before an 802.1X user enters the quiet state.

The **undo dot1x quiet-times** command restores the default setting.

By default, an 802.1X user enters the quiet state after ten authentication failures within 60 seconds.

Format

dot1x quiet-times *fail-times*

undo dot1x quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before the 802.1X user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the quiet timer function of the device is enabled using the **dot1x quiet-period** command, if the number of authentication failures of an 802.1X user exceeds the value that is set using the **dot1x quiet-times** command within 60 seconds, the user enters the quiet state. This prevents the impact on the system due to frequent user authentication.

Example

Set the maximum number of authentication failures within 60 seconds to 4.

```
<HUAWEI> system-view
[HUAWEI] dot1x quiet-times 4
```

13.6.79 dot1x reauthenticate

Function

The **dot1x reauthenticate** command enables periodic 802.1X re-authentication on an interface.

The **undo dot1x reauthenticate** command disables periodic 802.1X re-authentication on an interface.

By default, periodic 802.1X re-authentication is disabled on an interface.

Format

In the system view:

dot1x reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x reauthenticate

undo dot1x reauthenticate

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying the authentication information of an online user on the authentication server, the administrator needs to re-authenticate the user in real time to ensure user validity.

After the user goes online, the device saves user authentication information. After 802.1X re-authentication is enabled using the **dot1x reauthenticate** command, the device sends the stored authentication information of the online user to the authentication server for re-authentication at an interval. If the authentication information of the user does not change on the authentication server, the user is online normally. If the authentication information has been changed, the user is forced to go offline. The user then needs to be re-authenticated according to the changed authentication information.

NOTE

The re-authentication interval is set using the **dot1x timer reauthenticate-period** command.

This function takes effect only for users who go online after this function is successfully configured.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Precautions

If periodic 802.1X re-authentication is enabled, a large number of 802.1X authentication logs are generated.

Example

Enable periodic 802.1X re-authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x reauthenticate interface gigabitethernet 0/0/1
```

Enable periodic 802.1X re-authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x reauthenticate
```

13.6.80 dot1x reauthenticate mac-address

Function

The **dot1x reauthenticate mac-address** command enables re-authentication for an online 802.1X user with the specified MAC address.

By default, re-authentication is disabled for an online 802.1X user with the specified MAC address.

Format

dot1x reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of an 802.1X user to be re-authenticated.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **dot1x reauthenticate**.

The **dot1x reauthenticate mac-address** and **dot1x reauthenticate** commands re-authenticate online 802.1X users and their difference is as follows:

- The **dot1x reauthenticate mac-address** command configures the device to re-authenticate a specified user for once.
- The **dot1x reauthenticate** command configures the device to re-authenticate all users on a specified interface at intervals.
- The **dot1x reauthenticate mac-address** command does not support re-authentication for 802.1X users in pre-connection state.

Example

Enable re-authentication for an 802.1X user with the MAC address of 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] dot1x reauthenticate mac-address 00e0-fc12-3456
```

13.6.81 dot1x retry

Function

The **dot1x retry** command configures the number of times an authentication request is retransmitted to an 802.1X user.

The **undo dot1x retry** command restores the default configuration.

By default, the device can retransmit an authentication request to an 802.1X user twice.

Format

dot1x retry *max-retry-value*

undo dot1x retry

Parameters

Parameter	Description	Value
max-retry-value	Specifies the number of times an authentication request is retransmitted to an 802.1X user.	The value is an integer that ranges from 1 to 10. By default, the device can retransmit an authentication request to an 802.1X user twice. The default value is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the device does not receive any response from a user within a specified time after sending an authentication request to the user, the device sends the authentication request again. If the authentication request has been sent for the maximum retransmission times and no response is received, the user authentication fails. In this process, the total number of authentication requests sent by the device is *max-retry-value* plus 1.

NOTE

- After you run the **dot1x retry** command, the setting takes effect on all interfaces enabled with 802.1X authentication.
- Repeated authentication requests occupy a lot of system resources. When using the **dot1x retry** command, you can set the maximum number of times according to user requirements and device resources. The default value is recommended.
- The interval for sending authentication requests is set using the **dot1x timer** command. The interval for sending authentication requests to offline users is controlled by the **tx-period** and **client-timeout** timer, and the interval for sending authentication requests to online users is controlled by the **handshake-period** timer.
- The **dot1x retry** command is used together with the guest VLAN function (for details, see **authentication guest-vlan**). If a user does not respond within the specified maximum number of times, the user is added to the guest VLAN so that the user can access resources in the guest VLAN without being authenticated.

Example

Set the number of times an authentication request can be retransmitted to 802.1X users to 4.

```
<HUAWEI> system-view
[HUAWEI] dot1x retry 4
```

13.6.82 dot1x timer

Function

The **dot1x timer** command sets values of timers used in 802.1X authentication.

The **undo dot1x timer** command restores the default settings of timers used in 802.1X authentication.

For the default settings of timers used in 802.1X authentication, see the table in "Parameters".

Format

dot1x timer { **client-timeout** *client-timeout-value* | **quiet-period** *quiet-period-value* | **tx-period** *tx-period-value* | **mac-bypass-delay** *delay-time-value* | **free-ip-timeout** *free-ip-time-value* }

undo dot1x timer { **client-timeout** | **quiet-period** | **tx-period** | **mac-bypass-delay** | **free-ip-timeout** }

Parameters

Parameter	Description	Value
client-timeout *client-timeout-value*	Specifies the timeout interval of the authentication response from the client. You are advised to set this parameter to 30 seconds. **NOTE** On the network, some terminals may delay in responding to EAP-Request/MD5 Challenge packets sent from the device. If the delay is long, you can increase **client-timeout** *client-timeout-value* so that these terminals can go online. The adjustment rule is as follows: 3 x **client-timeout** *client-timeout-value* > Terminal response delay	The value is an integer that ranges from 1 to 120, in seconds. By default, the timeout interval of the authentication response from the client is 5 seconds.

Parameter	Description	Value
quiet-period *quiet-period-value*	Specifies the quiet period. For details, see **dot1x quiet-period**.	The value is an integer that ranges from 1 to 3600, in seconds. By default, the quiet period of a user who fails authentication is 60 seconds.
tx-period *tx-period-value*	Specifies the interval for sending authentication requests. The device starts the **tx-period** timer in either of the following situations: • When the client initiates authentication, the device sends a unicast Request/Identity request packet to the client and starts the **tx-period** timer. If the client does not respond within the period set by the timer, the device retransmits the authentication request packet. • To authenticate the 802.1X clients that cannot initiate authentication, the device sends multicast Request/Identity packets through the 802.1X-enabled interface to the clients at the interval set by the **tx-period** timer.	The value is an integer that ranges from 1 to 120, in seconds. By default, the interval for sending authentication requests is 30 seconds.

Parameter	Description	Value
mac-bypass-delay *delay-time-value*	Specifies the value of the delay timer for MAC address bypass authentication. After MAC address bypass authentication is configured, the device performs 802.1X authentication and starts the delay timer for MAC address bypass authentication. If 802.1X authentication fails after the value of the delay timer is reached, the device performs MAC address bypass authentication.	The value is an integer that ranges from 1 to 300, in seconds. By default, the value of the delay timer for MAC address bypass authentication is 30s.
free-ip-timeout *free-ip-time-value*	Specifies the aging time of authentication-free user entries. When the 802.1X free IP subnet is configured, the device creates authentication-free user entries after receiving ARP/DHCP packets from 802.1X users. If users go offline abnormally, the authentication-free user entries cannot be deleted. To prevent this problem, the aging time of authentication-free user entries can be configured.	The value is an integer that ranges from 0 to 71581, in minutes. The value 0 indicates that authentication-free user entries do not age. By default, the value of the aging time for authentication-free user entries is 1380 minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, multiple timers implement systematic interactions between access users, access devices, and the authentication server. You can

change the values of the timers using the **dot1x timer** command to adjust the interaction process. (The values of some timers cannot be changed.) This command is necessary in special network environments. Generally, the default settings of the timers are recommended.

Example

Set the timeout interval of the authentication response from the client to 90s.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer client-timeout 90
```

13.6.83 dot1x timer arp-detect

Function

The **dot1x timer arp-detect** command sets the timeout interval of the ARP detect.

The **undo dot1x timer arp-detect** command restores the default settings.

By default, the timeout interval of the ARP detect is 120 seconds.

Format

dot1x timer arp-detect *arp-detect-value*

undo dot1x timer arp-detect

Parameters

Parameter	Description	Value
arp-detect *arp-detect-value*	Specifies the timeout interval of the ARP detect.	The value is 0 or an integer that ranges from 5 to 7200, in seconds. 0 indicates that the ARP detect function is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The ARP probe function can also be implemented by detecting whether there is user traffic on the access device. If the ARP probe interval is **n**, the device detects user traffic at **n** and **2n**. The following uses the **0-n** period as an example. The

process during the **n-2n** period is the same as that during **0-n**. (This process applies only to users who go online from the S5731-H,?S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI. Other device models do not support user traffic detection, and they send ARP probe packets at **n** and **2n**.)

- If user traffic passes through the device within the **0-n** period, the device considers that the user is online at **n**, and will not send ARP probe packets. Additionally, the device resets the ARP probe interval.
- If no user traffic passes through the device within the **0-n** period, the device cannot determine whether the user is online at **n**. In this case, the device sends an ARP probe packet. If the device receives an ARP reply packet from the user, it considers the user online and resets the ARP probe interval. If no ARP reply packet is received, the device considers the user offline.
- If user traffic passes through the device or the device receives an ARP reply packet from the user within the **2n-3n** period, the device considers that the user is online at **3n** and resets the ARP probe interval.
- If no user traffic passes through the device and the device receives no ARP reply packet from the user within the **2n-3n** period, the device cannot determine whether the user is online at **3n** and considers the user offline.

If the device considers that the user is offline at **n**, **2n**, and **3n**, the device deletes all entries related to the user. To prevent the user from going offline unexpectedly when no operation is performed on the PC, do not set a short ARP probe interval.

Example

Set the timeout interval of the ARP detect to 90s.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer arp-detect 90
```

13.6.84 dot1x timer reauthenticate-period

Function

The **dot1x timer reauthenticate-period** command sets the re-authentication interval for 802.1X authentication users.

The **undo dot1x timer reauthenticate-period** command restores the default re-authentication interval.

By default, the re-authentication interval is 3600 seconds.

Format

dot1x timer reauthenticate-period *reauthenticate-period-value*

undo dot1x timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the re-authentication interval for 802.1X address authentication users. To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After enabling the re-authentication function for online 802.1X authentication users using the **dot1x reauthenticate** command, run the **dot1x timer reauthenticate-period** command to set the re-authentication interval. The device then authenticates online users at the specified interval, ensuring that only authorized users can keep online.

If the command is executed in the system view, the function takes effect on all interfaces. If the command is executed in both system view and interface view, the function takes effect on the interface.

NOTE

It is recommended that the re-authentication interval be set to the default value. If multiple ACLs need to be delivered during user authorization, you are advised to disable the re-authentication function or set a longer re-authentication interval to improve the device's processing performance.

In remote authentication and authorization, if the re-authentication interval is set to a shorter time, the CPU usage may be higher.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

Set the 802.1X re-authentication interval to 7200 seconds.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer reauthenticate-period 7200
```


13.6.85 dot1x trigger dhcp-binding

Function

The **dot1x trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication.

The **undo dot1x trigger dhcp-binding** command restores the default setting.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication.

Format

dot1x trigger dhcp-binding

undo dot1x trigger dhcp-binding

Parameters

None

Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Scenario

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through 802.1X authentication, the unauthorized users can obtain the same identities as the authorized users and connect to the network without authentication. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting normal communication between authorized users. To prevent the previous attacks, configure IPSG and DAI. These two functions are implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After the static IP users who pass 802.1X authentication send EAP packets to trigger generation of the user information table, the device automatically generates the DHCP snooping binding table based on the MAC address, IP address, and interface recorded in the table.

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass 802.1X authentication. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.
- In the interface view, run the **arp anti-attack check user-bind enable** command to enable DAI.

Precautions

- Before configuring the device to generate the DHCP snooping binding table for static IP users, you must have enabled 802.1X authentication and DHCP snooping globally and on interfaces using the **dot1x enable** and **dhcp snooping enable** commands.
- The EAP protocol does not specify a standard attribute to carry IP address information. Therefore, if the EAP request packet sent by a static IP user does not contain an IP address, the IP address information in the DHCP snooping binding table is obtained from the user' first ARP request packet with the same MAC address as the user information table after the user passes authentication. On a network, unauthorized users may forge authorized users' MAC addresses to initiate ARP snooping attacks to devices, and the DHCP snooping binding table generated accordingly may be unreliable. Therefore, the **dot1x trigger dhcp-binding** command is not recommended and you are advised to run the **user-bind static** command to configure the static binding table.
- For users who are assigned IP addresses using DHCP, you do not need to run the **dot1x trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function.

Example

Enable the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x trigger dhcp-binding
```

13.6.86 dot1x unicast-trigger

Function

The **dot1x unicast-trigger** command enables 802.1X authentication triggered by unicast packets.

The **undo dot1x unicast-trigger** command disables 802.1X authentication triggered by unicast packets.

By default, 802.1X authentication triggered by unicast packets is disabled.

Format

In the system view:

dot1x unicast-trigger interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x unicast-trigger interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x unicast-trigger

undo dot1x unicast-trigger

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After the **dot1x unicast-trigger** command is used on the device, the device sends a unicast packet to respond to the received ARP or DHCP Request packet from a client. If the client does not respond within the timeout interval (set by the **dot1x timer** command), the device retransmits the unicast packet (the maximum of retransmission count is set by the **dot1x retry** command). During 802.1X-based network deployment, 802.1X users can start 802.1X authentication without installing specified client dial-in software, which facilitates network deployment.

NOTE

The **dot1x unicast-trigger** command has the same function as the **dot1x dhcp-trigger** command.

Example

Enable 802.1X authentication triggered by unicast packets on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x unicast-trigger interface gigabitethernet 0/0/1
```

13.6.87 dot1x url

Function

The **dot1x url** command configures a redirect URL in 802.1X authentication.

The **undo dot1x url** command cancels the redirect URL configuration in 802.1X authentication.

By default, no redirect URL is configured in 802.1X authentication.

Format

dot1x url *url-string*

undo dot1x url

Parameters

Parameter	Description	Value
url-string	Specifies a redirect URL.	The value is a string of 1 to 247 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the early stage of network deployment, 802.1X client deployment is difficult and requires heavy workload. You can run the **dot1x url** command to set a redirect URL to the web page address for downloading the 802.1X client. When a user uses a browser to access resources that are not in the authentication-free IP subnet, the device redirects the URL that the user attempts to access to the 802.1X client download web URL after the device receives HTTP packets from the user. The user then can download and install the 802.1X client.

Follow-up Procedure

Run the **dot1x free-ip** command to configure the network segment where the redirect URL used in 802.1X authentication belongs or configure the IP address segment of the DNS server as an authentication-free IP subnet. To ensure that pre-connection users can be aged out normally, you need to run the **dot1x timer free-ip-timeout** command to set the aging time of authentication-free user entries.

Precautions

This command applies when users use the 802.1X client software that is not provided by the system.

The redirect URL must be within the authentication-free IP subnet. Otherwise, the URL will be inaccessible.

When 802.1X-based fast deployment is configured, the device supports redirection triggered only by HTTP packets with HTTP port 80.

Example

Set the redirect URL in 802.1X authentication to http://10.1.1.1:8080/download.

```
<HUAWEI> system-view
[HUAWEI] dot1x url http://10.1.1.1:8080/download
```

13.6.88 force-push

Function

The **force-push** command enables a pushed URL template or pushed URL.

The **undo force-push** command disables a pushed URL template or pushed URL.

By default, no pushed URL template or pushed URL is enabled.

Format

force-push { **url-template** *template-name* | **url** *url-address* }

undo force-push

Parameters

Parameter	Description	Value
url-template *template-name*	Specifies the name of a pushed URL template.	The value must be the name of an existing URL template.
url *url-address*	Specifies a pushed URL.	The value is a string of 1 to 247 case-sensitive characters without spaces and question marks (?). If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a user sends an HTTP/HTTPS packet to access a web page for the first time after the user is successfully authenticated, the device forcibly redirects the user to a specified web page. In addition to pushing advertisement pages, the device obtains user terminal information through the HTTP/HTTPS packets sent by users, and applies the information to other services. There are two ways to push web pages:

1. URL: pushes the URL of the specified web page.
2. URL template: pushes a URL template. The URL template must have been created and contains the URL of the pushed web page and URL parameters.

Prerequisites

The URL configured using the **url** command in the URL template view cannot be a redirect URL; otherwise, the **force-push** command does not take effect.

Precautions

For the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the forcible web page push function takes effect only for the first HTTP or HTTPS packet sent from users. If an application that actively sends HTTP or HTTPS packets is installed on a user terminal and the terminal has sent HTTP or HTTPS packets before the user accesses a web page, the user is unaware of the web page push process.

For switches except the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: The forcible web page push function takes

effect only when it is used together with a redirect ACL. If a redirect ACL exists in the user table, a web page is forcibly pushed when HTTP or HTTPS packets from users match the redirect ACL rule. Usually, you can configure the RADIUS server to authorize the Huawei extended RADIUS attribute **HW-Redirect-ACL** or **HW-IPv6-Redirect-ACL** to users for redirect ACL implementation, or run the **redirect-acl** command to configure a redirect ACL.

A pushed URL configured in a domain needs to be used together with a redirect ACL or push flag attribute. The redirect ACL has a higher priority than the push flag attribute. By default, a pushed URL configured in a domain carries the push flag attribute. Users will be redirected to the pushed URL when they are successfully authenticated.

When an IPv4 redirect ACL is configured for an IPv6 user or an IPv6 redirect ACL is configured for an IPv4 user, the **Push URL content** field in the **display access-user** command output displays the pushed URL, but the browser of the user cannot redirect to the pushed URL.

Switches except the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support concurrent use of the pushed URL and redirection ACL6 functions. If both functions are configured, the **Push URL content** field in the **display access-user** command output displays the pushed URL; however, the terminal browser cannot be redirected to the pushed URL.

Example

Enable the pushed URL template **abc** in the domain **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] force-push url-template abc
```

13.6.89 http get-method enable

Function

The **http get-method enable** command configures the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

The **undo http get-method enable** command restores the default setting.

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication.

Format

http get-method enable

undo http get-method enable

Parameters

None

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication. You can run the **http get-method enable** command to configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

Precautions

The GET mode has the risk of password disclosure. Therefore, the POST mode is recommended.

This command only applies to scenarios in which HTTP or HTTPS is used for Portal connection establishment.

Example

Configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] http get-method enable
```

13.6.90 http-method post

Function

The **http-method post** command configures parameters for parsing and replying to POST request packets of the HTTP or HTTPS protocol.

The **undo http-method post** command restores the default configuration.

By default, the system has configured parameters for parsing and replying to POST request packets of the HTTP or HTTPS protocol. For details, see the "Parameters" table.

Format

http-method post { **cmd-key** *cmd-key* [**login** *login-key* | **logout** *logout-key*] * | **init-url-key** *init-url-key* | **login-fail response** { **err-msg** { **authenserve-reply-message** | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] } | **login-success response** { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* } | **logout-fail response** { **msg** *msg* | **redirect-url** *redirect-url* } | **logout-success response** { **msg** *msg* | **redirect-url** *redirect-url* } |

password-key *password-key* | **user-mac-key** *user-mac-key* | **userip-key** *userip-key* | **username-key** *username-key* } *

undo http-method post { **all** | { **cmd-key** | **init-url-key** | **login-fail** | **login-success** | **logout-fail** | **logout-success** | **password-key** | **user-mac-key** | **userip-key** | **username-key** } * }

Parameters

Parameter	Description	Value
cmd-key *cmd-key*	Specifies the command identification keyword. The default value is **cmd**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
login *login-key*	Specifies the user login identification keyword. The default value is **login**.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
logout *logout-key*	Specifies the user logout identification keyword. The default value is **logout**.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
init-url-key *init-url-key*	Specifies the identification keyword for the user initial login URL. The default value is **initurl**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
login-fail response { **err-msg** { **authenserve-reply-message** | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] }	Specifies the response message upon a user login failure. • **err-msg authenserve-reply-message**: The response message returned by the authentication server is displayed upon a user login failure. • **err-msg msg** *msg*: A specified message is displayed upon a user login failure. • **redirect-login-url**: A user is redirected to the login URL upon a login failure. This mode is used by default. • **redirect-url** *redirect-url*: A user is redirected to a specified URL upon a login failure. • **append-reply-message** *msgkey*: The redirect URL carries the identification keyword for the response message returned by the authentication server.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces. • *msgkey*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
login-success response { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* }	Specifies the response message upon successful user login. • **msg** *msg*: A specified message is displayed upon successful user login. • **redirect-init-url**: A user is redirected to the initial login URL upon successful login. This mode is used by default. • **redirect-url** *redirect-url*: A user is redirected to a specified URL upon successful login.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).
logout-fail response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon a user logout failure. • **msg** *msg*: A specified message is displayed upon a user logout failure. The default value is **LogoutFail!**. • **redirect-url** *redirect-url*: A user is redirected to a specified URL upon a logout failure.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).
logout-success response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon successful user logout. • **msg** *msg*: A specified message is displayed upon successful user logout. The default value is **LogoutSuccess!**. • **redirect-url** *redirect-url*: A user is redirected to a specified URL upon successful logout.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).

Parameter	Description	Value
password-key *password-key*	Specifies the password identification keyword. The default value is **password**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
user-mac-key *user-mac-key*	Specifies the identification keyword for the user MAC address. The default value is **macaddress**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
userip-key *userip-key*	Specifies the identification keyword for the user IP address. The default value is **ipaddress**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
username-key *username-key*	Specifies the user name identification keyword. The default value is **username**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
all	Indicates all parameters.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

When the device uses the HTTP or HTTPS protocol to communicate with the Portal server, a user sends POST request packets (carrying parameters such as the user name and MAC address) to the device as required by the Portal server. After receiving the POST request packets, the device parses parameters in the packets. If identification keywords of the parameters differ from those configured on the device, the user authentication fails. Therefore, you need to run the **http-method post** command to configure the identification keywords based on the Portal server configuration.

After successful user login or logout, or a user login or logout failure, the device sends the login or logout result to the user based on the **http-method post**

command configuration. For example, the device sends the **LogoutSuccess!** message to a user who logs out successfully by default.

Example

Set the command identification keyword to **cmd1** for parsing POST request packets of the HTTP or HTTPS protocol.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] http-method post cmd-key cmd1
```

13.6.91 link-down offline delay

Function

The **link-down offline delay** command configures the user logout delay when an interface link is faulty.

The **undo link-down offline delay** command restores the default configuration.

By default, the user logout delay is 10 seconds when an interface link is faulty.

Format

link-down offline delay { *delay-value* | **unlimited** }

undo link-down offline delay

Parameters

Parameter	Description	Value
delay-value	Specifies the user logout delay when an interface link is faulty.	The value is an integer that ranges from 0 to 60, in seconds. If the value is 0, users are logged out immediately when an interface link is faulty.
unlimited	Indicates that users are not logged out when an interface link is faulty.	-

Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a link is faulty, the interface is interrupted and users are directly logged out. To solve this problem, you can configure the user logout delay function. When the interface link is faulty, the users remain online within the delay. In this case, if the link is restored, the users do not need to be re-authenticated. If the users are disconnected after the delay and the link is restored, the users need to be re-authenticated.

Precautions

- This function takes effect only for wired users who go online on Layer 2 physical interfaces that have been configured with NAC authentication.
- To make the function take effect, it is recommended that the configured interval be greater than the time during which the interface is in Up state. If the link frequently flaps within a short period, it is recommended that the interval be set to **unlimited**.

Example

Configure the user logout delay to 5 seconds when the link of GE0/0/1 is faulty.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] link-down offline delay 5
```

13.6.92 mac-authen

Function

The **mac-authen** command enables MAC address authentication globally or on an interface.

The **undo mac-authen** command disables MAC address authentication globally or on an interface.

By default, MAC address authentication is disabled globally and on an interface.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support configuration of MAC address authentication on VLANIF interfaces.

Format

In the system view:

mac-authen [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

undo mac-authen [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

In the interface view:

mac-authen

undo mac-authen

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MAC address authentication controls network access rights of a user based on the user's access interface and MAC address. During MAC address authentication, the user name and password are the user's MAC address. MAC address authentication is applicable to the scenario where MAC addresses are unchanged and high

security is not required, and is used to authenticate terminals such as printers where the authentication client cannot be installed.

If you run the **mac-authen** command in the system view without any interfaces specified, MAC address authentication is enabled globally. The configurations of MAC address authentication take effect only after global MAC address authentication is enabled. MAC address bypass authentication is not controlled by this command.

To enable MAC address authentication on an interface, you can perform either of the following operations:

- Run the **mac-authen** command in the interface view.
- Run the **mac-authen interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> command in the system view.

Precautions

- Before running the **undo mac-authen** command, ensure that there is no online MAC address authentication user; otherwise, you cannot run this command. Online MAC address authentication users do not include online users using MAC address bypass authentication.
- After MAC address authentication is enabled on a VLANIF interface, the guest VLAN, critical VLAN, or dynamic VLAN authorization is invalid to the MAC address authentication users on the VLANIF interface.
- Before enabling MAC address authentication on the VLANIF interface, ensure that the strict ARP entry learning function is disabled using the **undo arp learning strict** command. If the function is enabled, the users cannot go online.
- After the static MAC address entry is configured using the **mac-address static** *mac-address interface-type interface-number* **vlan** *vlan-id* command, the user corresponding to the entry cannot pass MAC address authentication.
- If MAC address authentication is enabled on an interface, the following commands cannot be used on the same interface. If the following commands are configured on an interface, MAC address authentication cannot be enabled on the same interface.

Command	Function
mac-limit	Sets the maximum number of MAC addresses that can be learned by an interface.
mac-address learning disable	Disables MAC address learning on an interface.
port link-type dot1q-tunnel	Sets the link type of an interface to QinQ.
port vlan-mapping vlan map-vlan **port vlan-mapping vlan inner-vlan**	Configures VLAN mapping on an interface.
port vlan-stacking	Configures selective QinQ.

Command	Function
mac-vlan enable	Enables MAC address-based VLAN assignment on an interface.
ip-subnet-vlan enable	Enables IP subnet-based VLAN assignment on an interface.
user-bind ip sticky-mac	Enables the device to generate snooping MAC entries.

Example

Enable global MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] mac-authen
```

Enable MAC address authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen
[HUAWEI] mac-authen interface gigabitethernet 0/0/1
```

Enable MAC address authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen
```

13.6.93 mac-authen trigger

Function

The **mac-authen trigger** command configures the packet types that can trigger MAC address authentication.

The **undo mac-authen trigger** command restores the default configuration.

By default, DHCP/ARP/DHCPv6/ND packets can trigger MAC address authentication.

Format

In the system view:

mac-authen { **dhcp-trigger** | **arp-trigger** | **dhcpv6-trigger** | **nd-trigger** } * [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

undo mac-authen { **dhcp-trigger** | **arp-trigger** | **dhcpv6-trigger** | **nd-trigger** } * [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

In the interface view:

mac-authen { **dhcp-trigger** | **arp-trigger** | **dhcpv6-trigger** | **nd-trigger** } *

undo mac-authen { **dhcp-trigger** | **arp-trigger** | **dhcpv6-trigger** | **nd-trigger** } *

Parameters

Parameter	Description	Value
dhcp-trigger	Triggers MAC address authentication through DHCP packets.	-
arp-trigger	Triggers MAC address authentication through ARP packets.	-
dhcpv6-trigger	Triggers MAC address authentication through DHCPv6 packets.	-
nd-trigger	Triggers MAC address authentication through ND packets.	-
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. If this parameter is not specified, the command takes effect on all interfaces.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MAC address authentication is enabled, the device can trigger MAC address authentication on users by default when receiving DHCP/ARP/DHCPv6/ND packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger MAC address authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger MAC address authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger MAC address authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

Precautions

If the command is configured globally, the configuration takes effect on multiple interfaces. If the command is configured globally and on an interface, the configuration on the interface takes precedence.

The **mac-authen trigger** command also enables MAC address authentication. When both the **mac-authen trigger** and **mac-authen** commands are configured on an interface, the last configured one takes effect. If the **mac-authen** configuration takes effect on the interface, DHCP, ARP, DHCPv6, and ND packets can trigger MAC address authentication.

Example

Configure the device to trigger MAC address authentication only through DHCP packets in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen dhcp-trigger
```

13.6.94 mac-authen dhcp-trigger dhcp-option

Function

The **mac-authen dhcp-trigger dhcp-option** command enables the device to send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

The **undo mac-authen dhcp-trigger dhcp-option** command restores the default configuration.

By default, the device does not send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

Format

In the system view:

mac-authen dhcp-trigger dhcp-option *option-code* [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

undo mac-authen dhcp-trigger dhcp-option *option-code* [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

In the interface view:

mac-authen dhcp-trigger dhcp-option *option-code*

undo mac-authen dhcp-trigger dhcp-option *option-code*

Parameters

Parameter	Description	Value
option-code	Specifies the option that the device sends to the authentication server.	The value is fixed as 82.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Option82 record information about DHCP user locations and services (voice and data services). After this command is run, if the device supports the function of

triggering MAC address authentication through DHCP packets, it sends Option82 information to the authentication server when triggering MAC address authentication through DHCP packets. Based on the user information recorded in Option82, the authentication server then assigns different network access rights to users with different services in different locations. This implements accurate control on the network access right of each user.

Example

Globally enable the device to send Option82 information to the authentication server when triggering MAC address authentication through DHCP packets.

```
<HUAWEI> system-view
[HUAWEI] mac-authen dhcp-trigger dhcp-option 82
```

13.6.95 mac-authen domain

Function

The **mac-authen domain** command configures an authentication domain for MAC address authentication users.

The **undo mac-authen domain** command restores the global default authentication domain for MAC address authentication users.

The default authentication domain for MAC address authentication users is the global default domain.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support configuration of MAC address authentication on VLANIF interfaces.

Format

In the system view:

mac-authen domain *isp-name* [**mac-address** *mac-address* **mask** *mask*]

undo mac-authen domain [*isp-name* [**mac-address** *mac-address*] | [**mac-address** { *mac-address* | **all** }]]

In the interface view:

mac-authen domain *isp-name*

undo mac-authen domain

Parameters

Parameter	Description	Value
isp-name	Specifies the ISP domain name.	The value is a string of 1 to 64 case-insensitive characters without any space, asterisk (*), question mark (?), quotation mark ("), hyphen (-) or consecutive hyphens (--).
mac-address *mac-address*	Specifies an authentication domain for the MAC address authentication user with a specified MAC address. **NOTE** A maximum of 16 MAC address ranges can be specified.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the mask of a MAC address.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
all	Restores the global default domain for all MAC address authentication users.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When user names for MAC address authentication do not contain domain names, the device authenticates users using the **default** domain if no authentication domain is configured on the device or interface. The authentication scheme is not flexible because all users are authenticated in the **default** domain. The **mac-authen domain** command specifies the authentication domains for MAC address authentication users. Different interfaces can be located in different authentication domains. This command can specify the authentication domains

for the specified MAC addresses. Therefore, this command allows users with different authentication requirements to adopt various authentication schemes.

NOTE

- If the user name contains a domain name (configured using **mac-authen username**), the user is authenticated in this domain.
- The specified user names and domain names must be the same as those configured in the AAA view.
- The authentication schemes in the domains are configured in the AAA view.

Prerequisites

The domain to be configured as an authentication domain has been created using the **domain (AAA view)** command.

MAC address authentication has been enabled globally and on an interface using the **mac-authen** command.

Precautions

If authentication domains are configured in both the system view and interface view, the domain configured in the interface view takes effect. If no authentication domain is configured in the interface view, the domain configured in the system view takes effect.

You must specify a unicast MAC address in the **mac-authen domain** command. A user with an all-0 MAC address is not authenticated.

The configured authentication domain is applied to the MAC addresses calculated with the mask. Therefore, the **undo mac-authen domain** command will delete the authentication domain of the calculated MAC addresses. Before running the **undo mac-authen domain** command, run the **display this** command to view the calculated MAC addresses.

On a network configured with both 802.1X authentication and MAC address bypass authentication, an 802.1X user failing the 802.1X authentication will be authenticated in the manner of MAC address bypass authentication. If the authentication scheme of MAC address bypass authentication is none authentication, the user can go online successfully without being authenticated. To prevent such unauthorized authentication, use the **mac-authen domain** command to specify different domains for the two authentication methods.

Example

Configure the **cams** domain as the authentication domain for MAC address authentication users in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen domain cams
```

Configure the **cams** domain as the authentication domain for MAC address authentication users in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen domain cams
```


13.6.96 mac-authen max-user

Function

The **mac-authen max-user** command sets the maximum number of MAC address authentication users on an interface.

The **undo mac-authen max-user** command restores the default value of the maximum number of MAC address authentication users on an interface.

By default, the number of MAC address authentication users is the maximum number of MAC address authentication users supported by the device.

Format

In the system view:

mac-authen max-user *user-number* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen max-user [*user-number*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen max-user *user-number*

undo mac-authen max-user [*user-number*]

Parameters

Parameter	Description	Value
user-number	Specifies the maximum number of MAC address authentication users on an interface.	The value is an integer that varies depending on the product model.

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To limit the number of MAC address authentication users on an interface, run the **mac-authen max-user** command. When the number of access users on an interface reaches the limit, the device will not trigger authentication for the users newly connected to the interface; therefore, these users cannot access the network.

Prerequisites

MAC address authentication has been enabled globally and on an interface using the **mac-authen** command.

Example

Set the maximum number of MAC address authentication users on GE0/0/1 to 8 in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen max-user 8 interface gigabitethernet 0/0/1
```

Set the maximum number of MAC address authentication users on GE0/0/1 to 8 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen max-user 8
```

13.6.97 mac-authen offline dhcp-release

Function

The **mac-authen offline dhcp-release** command enables the device to clear user entries when receiving DHCP Release packets from MAC address authentication users.

The **undo mac-authen offline dhcp-release** command restores the default configuration.

By default, the device does not clear user entries when receiving DHCP Release packets from MAC address authentication users.

Format

In the system view:

mac-authen offline dhcp-release interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen offline dhcp-release interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen offline dhcp-release

undo mac-authen offline dhcp-release

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. *interface-number2* and *interface-number1* together specify an interface range.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MAC address authentication users who send DHCP Release packets go offline, the corresponding user entries on the device cannot be deleted immediately. This occupies device resources and possibly prevents other users from going online. You can run this command to enable the device to clear the user entries in real time when MAC address authentication users go offline.

Precautions

If the device functions as a DHCP relay agent, configure the DHCP snooping function on the device; otherwise, this command does not take effect.

Example

In the system view, enable the device to clear user entries when receiving DHCP Release packets from MAC address authentication users on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mac-authen offline dhcp-release interface gigabitethernet 0/0/1
```

In the interface view, enable the device to clear user entries when receiving DHCP Release packets from MAC address authentication users on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen offline dhcp-release
```

13.6.98 mac-authen permit mac-address

Function

The **mac-authen permit mac-address** command specifies the MAC address range allowed for MAC address authentication.

The **undo mac-authen permit mac-address** command deletes the MAC address range allowed for MAC address authentication.

By default, no MAC address range is specified for MAC address authentication.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

undo mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address for MAC address authentication.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the MAC address mask.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask-length*	Specifies the MAC address mask length.	The value is an integer that ranges from 1 to 48.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

By default, any new MAC address is allowed for MAC address authentication after MAC address authentication is enabled on a VLANIF interface. To actually control the users who can be authenticated using MAC addresses on the VLANIF interface, use this command to specify a MAC address range for MAC address authentication.

Example

Set the MAC address to 00e0-fc01-0101 and the MAC address mask length to 24 for MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 10
[HUAWEI-Vlanif10] mac-authen permit mac-address 00e0-fc01-0101 mask 24
```

13.6.99 mac-authen quiet-times

Function

The **mac-authen quiet-times** command configures the maximum number of authentication failures within 60 seconds before a MAC authentication user enters the quiet state.

The **undo mac-authen quiet-times** command restores the maximum number of authentication failures to the default value.

By default, the maximum number of authentication failures is 10.

Format

mac-authen quiet-times *fail-times*

undo mac-authen quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a MAC authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The quiet function for MAC address authentication is enabled on a device by default. When the maximum number of authentication failures exceeds 1, the device quiets a MAC authentication user and does not process authentication requests from the user, reducing impact on the system caused by attackers.

Precautions

After the maximum number of authentication failures is set to a value larger than the configured value, the user in quiet state can initiate reauthentication only after the quiet period expires. If the user enters an incorrect user name or password again, the user authentication fails. The device does not quiet the user but allows the user to initiate reauthentication immediately.

Example

Set the maximum number of authentication failures within 60 seconds to 4.

```
<HUAWEI> system-view
[HUAWEI] mac-authen quiet-times 4
```

13.6.100 mac-authen reauthenticate

Function

The **mac-authen reauthenticate** command enables periodic MAC address re-authentication on a specified interface.

The **undo mac-authen reauthenticate** command disables periodic MAC address re-authentication on a specified interface.

By default, periodic MAC address re-authentication is enabled on a specified interface.

Format

In the system view:

mac-authen reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen reauthenticate

undo mac-authen reauthenticate

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After modifying the authentication information of an online user on the authentication server, the administrator needs to re-authenticate the user in real time to ensure user validity.

After the user goes online, the device saves user authentication information. After periodic re-authentication for all online MAC address authentication users on a

specified interface is enabled using the **mac-authen reauthenticate** command, the device sends the stored authentication information of the online user on the interface to the authentication server for re-authentication at an interval. If the user's authentication information does not change on the authentication server, the user is online normally. If the authentication information has been changed, the user is forced to go offline. The user then needs to be re-authenticated according to the changed authentication information.

NOTE

The re-authentication interval is set using the **mac-authen timer reauthenticate-period** command.

This function takes effect only for users who go online after this function is successfully configured.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Example

Enable periodic MAC address re-authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen reauthenticate interface gigabitethernet 0/0/1
```

Enable periodic MAC address re-authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen reauthenticate
```

13.6.101 mac-authen reauthenticate dhcp-renew

Function

The **mac-authen reauthenticate dhcp-renew** command enables the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

The **undo mac-authen reauthenticate dhcp-renew** command restores the default setting.

By default, the device does not re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

Format

In the system view:

mac-authen reauthenticate dhcp-renew interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen reauthenticate dhcp-renew interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen reauthenticate dhcp-renew

undo mac-authen reauthenticate dhcp-renew

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. *interface-number2* and *interface-number1* together specify an interface range.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After users go online, the administrator may modify the users' authentication parameters or network access rights on the authentication server. To ensure user validity or update the users' network access rights in real time, you can run this command to enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

NOTE

This function applies only to L2 BNG scenarios.

Example

In the system view, enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mac-authen reauthenticate dhcp-renew interface gigabitethernet 0/0/1
```

In the interface view, enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen reauthenticate dhcp-renew
```

13.6.102 mac-authen reauthenticate mac-address

Function

The **mac-authen reauthenticate mac-address** command enables re-authentication for an online MAC address authentication user with a specified MAC address.

By default, re-authentication for an online MAC address authentication user with a specified MAC address is disabled.

Format

mac-authen reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies all valid unicast MAC addresses.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **mac-authen reauthenticate**.

The **mac-authen reauthenticate mac-address** and **mac-authen reauthenticate** commands re-authenticate online MAC address authentication users and their difference is as follows:

- The **mac-authen reauthenticate mac-address** command configures the device to immediately re-authenticate a user with a specified MAC address for once.
- The **mac-authen reauthenticate** command configures the device to re-authenticate all online MAC address authentication users on a specified interface at intervals.
- The **mac-authen reauthenticate mac-address** command does not support re-authentication for MAC address authentication users in pre-connection state.

Example

Enable re-authentication for an online MAC address authentication user with the MAC address 00e0-fc02-0003.

```
<HUAWEI> system-view
[HUAWEI] mac-authen reauthenticate mac-address 00e0-fc02-0003
```

13.6.103 mac-authen timer

Function

The **mac-authen timer** command configures parameters of timers for MAC address authentication.

The **undo mac-authen timer** command restores the default parameter values of timers for MAC address authentication.

Format

mac-authen timer { **guest-vlan reauthenticate-period** *interval* | **offline-detect** *offline-detect-value* | **quiet-period** *quiet-value* }

undo mac-authen timer { **guest-vlan reauthenticate-period** | **offline-detect** | **quiet-period** }

Parameters

Parameter	Description	Value
guest-vlan reauthenticate-period *interval*	Specifies the interval for re-authenticating users in the Guest VLAN.	The value is an integer that ranges from 60 to 3600, in seconds. The default value is 60.

Parameter	Description	Value
offline-detect *offline-detect-value*	Specifies the interval for detecting online users. The timer is used to periodically check whether a user is offline. **NOTE** The timer takes effect for both MAC address authentication users and static users.	The value is an integer that ranges from 30 to 7200, and 0, in seconds. The default value is 300. 0 means disable detecting online users.
quiet-period *quiet-value*	Specifies the value of the quiet timer. If a user fails authentication, the device does not process the user's authentication requests until the quiet timer expires. During the quiet period, the device does not process the user's authentication requests.	The value is an integer that ranges from 0 to 3600, in seconds. By default, the quiet period of a user who fails authentication is 60 seconds. **NOTE** When the quiet timer is set to 0, the quiet function is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

During MAC address authentication, multiple timers implement systematic interactions between access users or devices and the authentication server. You can change the values of the timers by running the **mac-authen timer** command to adjust the interaction process. (The values of some timers cannot be changed.) This command is necessary in special network environments. Generally, the default settings of the timers are recommended.

NOTE

If the number of offline detection packets (ARP packets) exceeds the default CAR value, the detection fails and the users are logged out. (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.) To resolve the problem, the following methods are recommended:

- Increase the detection interval based on the number of users. The default detection interval is recommended when there are less than 8000 users; the detection interval should be no less than 600 seconds when there are more than 8000 users.
- Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

Example

Set the value of the quiet timer to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-authen timer quiet-period 60
```

13.6.104 mac-authen timer reauthenticate-period

Function

The **mac-authen timer reauthenticate-period** command sets the re-authentication interval for MAC address authentication users.

The **undo mac-authen timer reauthenticate-period** command restores the default re-authentication interval.

The default re-authentication interval for MAC address authentication users in the system view is 1800 seconds, and the re-authentication interval in the interface view is the same as the re-authentication interval configured in the system view.

Format

mac-authen timer reauthenticate-period *reauthenticate-period-value*

undo mac-authen timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the re-authentication interval for MAC address authentication users.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After enabling the re-authentication function for online MAC address authentication users using the **mac-authen reauthenticate** command, run the **mac-authen timer reauthenticate-period** command to set the re-authentication interval. The device then authenticates online users at the specified interval, ensuring that only authorized users can keep online.

If the command is executed in the system view, the function takes effect on all interfaces. If the command is executed in both system view and interface view, the function takes effect on the interface.

NOTE

It is recommended that the re-authentication interval be set to the default value. If multiple ACLs need to be delivered during user authorization, you are advised to disable the re-authentication function or set a longer re-authentication interval to improve the device's processing performance.

In remote authentication and authorization, if the re-authentication interval is set to a shorter time, the CPU usage may be higher.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

Set the re-authentication interval for online MAC address authentication users to 3600 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-authen timer reauthenticate-period 3600
```

13.6.105 mac-authen username

Function

The **mac-authen username** command configures the user name format for MAC address authentication.

The **undo mac-authen username** restores the default user name format.

By default, the MAC address without hyphens (-) or colons (:) is used as the user name and password for MAC address authentication.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support configuration of MAC address authentication on VLANIF interfaces.

Format

mac-authen username { **fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]] | **dhcp-option** *option-code* { **circuit-id** | **remote-id** } * [**separate** *separate*] [**format-hex**] **password cipher** *password* }

undo mac-authen username [**fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]] | **dhcp-option** *option-code* [**password cipher** *password*]]

Parameters

Parameter	Description	Value
fixed *username*	Specifies the fixed user name for MAC address authentication.	The value is a string of 1 to 64 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
password cipher *password*	Specifies the password displayed in cipher text for MAC address authentication. • The user with a fixed name can log in without a password if no password is set. This brings a security risk and is not recommended. • When a MAC address is used as the user name, the MAC address can be used as the password if no password is set. When local authentication is specified in the AAA authentication scheme, you must set a password. • If the DHCP option is used as the user name, you must set a password. **NOTE** If fixed user names are configured in the VLANIF interface view, Eth-Trunk interface view or port group view, the password must be set. If a MAC address is configured as the user name in the port group view, the password cannot be set.	The value is a case-sensitive string without question marks (?) or spaces. The password contains 1 to 128 characters in plain text or 48 to 188 characters in cipher text. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** For security purposes, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

Parameter	Description	Value
macaddress	Specifies that the user name in MAC address authentication is the MAC address.	-
format { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** }	Specifies the MAC address format. • **with-hyphen**: indicates that the MAC address contains hyphens (-), for example, 00e0-fc1c-02e3. • **with-hyphen normal**: indicates that the MAC address contains hyphens (-), for example, 00-e0-fc-1c-02-e3. • **with-hyphen colon**: indicates that the MAC address contains colons (:), for example, 00e0:fc1c:02e3. • **with-hyphen normal colon**: indicates that the MAC address contains colons (:), for example, 00:e0:fc:1c:02:e3. • **without-hyphen**: indicates that the MAC address does not contain hyphens (-) or colons (:), for example, 00e0fc1c02e3.	-
uppercase	Indicates that the name of a MAC address authentication user is in uppercase.	-

Parameter	Description	Value
dhcp-option *option-code*	Specifies the name of the MAC address authentication user to a specified DHCP option. • **circuit-id**: Specifies the circuit ID in the DHCP Option82 field as the user name in MAC address authentication. • **remote-id**: Specifies the remote ID in the DHCP Option82 field as the user name in MAC address authentication. If both **circuit-id** and **remote-id** are configured, the user name for MAC address authentication can be set to a character string that is a combination of the **circuit-id** and **remote-id** in the DHCP Option82 field. **NOTE** In VLANIF interface view, the parameter does not support.	The value is an integer. In the current version, the value is fixed as 82.
separate *separate*	Specifies the delimiter in the user name for MAC address authentication. This parameter is configured when the user name for MAC address authentication is set to a character string that is a combination of the **circuit-id** and **remote-id** in the DHCP Option82 field.	The value is a character and can be set to a letter, digit, or another valid character.
format-hex	Indicates that the user name for MAC address authentication is in hexadecimal format.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

MAC address authentication uses three user name formats:

- When the MAC address is used as the user name for MAC address authentication, the password can be the MAC address or a self-defined character string.
- When the fixed user name is used for MAC address authentication, the user uses the fixed user name and password set by the administrator for authentication.
- When the DHCP option format is used for MAC address authentication, the device uses the DHCP option it obtains and password set by the administrator for authentication. In this mode, ensure that the device supports MAC address authentication triggered through DHCP packets.

By default, the device uses the user's MAC address as the user name and password, and sends the MAC address to the authentication server for authentication. Therefore, it is inconvenient to identify and manage users. You can run the **mac-authen username** command to configure the fixed name and password for MAC address authentication users, which facilities user identification and management.

NOTE

When the user names for MAC address authentication are in the DHCP option format, the DHCP Option82 cannot be configured in the extend format or a customized format (non-character string) by using the **dhcp option82 format** command.

When the user name format in MAC address authentication is configured, ensure that the authentication server supports this format.

Example

Configure the user name to **vipuser** and the password to **pass123** for MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] mac-authen username fixed vipuser password cipher pass123
```

13.6.106 parameter

Function

The **parameter** command configures the characters used in URL.

The **undo parameter** command restores the default settings.

By default, the start character of URL parameters is a question mark (?), the assignment character of URL parameters is an equal sign (=), and the delimiter between URL parameters is an ampersand (&).

Format

parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

undo parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

Parameters

Parameter	Description	Value
start-mark *parameter-value*	Specifies the start character for URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
assignment-mark *parameter-value*	Specifies the assignment character for URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
isolate-mark *parameter-value*	Specifies the delimiter between URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

You can run the **parameter** command to modify the characters in URLs.

For example, in a Portal server template, a user with IP address 10.1.1.11 and MAC address 00e0-fc02-0002 is configured to be authenticated by an access device with

the system name of **test**. By default, the start character of URL parameters is a question mark (?), the assignment character of URL parameters is an equal sign (=), and the delimiter between URL parameters is an ampersand (&). When default settings are used, the access device redirects the user to the URL http://10.1.1.1?user_mac=00e0-fc02-0002&user_ip=10.1.1.11&sysname=test. However, the device does not support question marks (?) in the **url (URL template view)** command configuration. To resolve this problem, replace the question mark (?) in the URL with another character in the **url (URL template view)** configuration, and run the **parameter start-mark** *parameter-value* command to specify this replacement character as the start character of URL parameters. In the following example, the replacement character is a number sign (#).

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.1#user_mac=00e0-fc02-0002&user_ip=10.1.1.11&sysname=test
[HUAWEI-url-template-test] parameter start-mark #
```

Alternatively, you can run the **url** command in the URL template view to set the URL to **http://10.1.1.1**, and run the **url-parameter** command to add parameters such as the user MAC address, user IP address, and device system name to the URL. In this case, the **parameter** command does not need to be configured.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.1
[HUAWEI-url-template-test] url-parameter sysname test user-ipaddress 10.1.1.11 user-mac 00e0-fc02-0002
```

Example

Set the start character for URL parameters to a number sign (#).

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] parameter start-mark #
```

13.6.107 port connection-type access

Function

The **port connection-type access** command configures the specified interfaces as downlink interfaces.

The **undo port connection-type access** command configures the specified interfaces as uplink interfaces.

Format

port { *interface-type start-interface-number* [**to** *interface-type end-interface-number*] } &<1-10> **connection-type access**

undo port { *interface-type start-interface-number* [**to** *interface-type end-interface-number*] } &<1-10> **connection-type access**

Parameters

Parameter	Description	Value
interface-type start-interface-number [**to** *interface-type end-interface-number*]	Specifies interfaces. • *interface-type* specifies the interface type. • *start-interface-number* specifies the number of the first interface. • *end-interface-number* specifies the number of the last interface. If the **to** *interface-type end-interface-number* parameter is not specified, only the interfaces specified by *start-interface-number* are created. You can specify 10 interface ranges at one time.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, downlink interfaces are access ones and uplink interfaces are non-access ones. You can run the **port connection-type access** or **undo port connection-type access** command to modify the interface access type. For example, you can batch configure the downlink interfaces supported by the device, and run the **dot1x mac-bypass access-port** command to enable MAC address bypass authentication on all the downlink interfaces.

After the default interface access type is modified, the device generates the interface buildrun information in the system view.

Precautions

If stack interface information exists within the interface range, the command does not take effect. Therefore, there should be no interface with stack configuration in the interface range. If the access type of an interface is changed, stack

configuration cannot be performed for the interface. That is, if an interface needs to be configured as a stack interface, the default interface access type cannot be modified.

Example

Configure interfaces as downlink interfaces in the system view.

```
<HUAWEI> system-view
[HUAWEI] port GigabitEthernet 0/0/1 to GigabitEthernet 0/0/6 connection-type access
```

13.6.108 port (Portal server template view)

Function

The **port** command sets the port number that a Portal server uses to receive notification packets from the device.

The **undo port** command restores the default port number.

By default, a Portal server uses port number 50100 to receive packets from the device.

Format

port *port-number* [**all**]

undo port [**all**]

Parameters

Parameter	Description	Value
port-number	Specifies the port number that the Portal server uses to receive and encapsulate UDP packets from the device.	The value is an integer that ranges from 1 to 65535. By default, the value is 50100.
all	Indicates that the device always uses the destination port number specified by **port-number** to encapsulate UDP packets. **NOTE** After this keyword is specified, when receiving UDP packets from a Portal server, the device does not obtain the source port number in the UDP packets as the destination port number of UDP packets to be sent to the Portal server. If the value of *port-number* is different from the source port number of the Portal server, the Portal server cannot receive the UDP packets sent by the device. Therefore, this keyword is not recommended.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server template on the device using the **web-auth-server** command, configure parameters for the template.

Run the **port** command to set the port number that a Portal server uses to receive notification packets from the device. After receiving a Portal authentication request packet from a user, the device sends the packet to the Portal server using the specified destination port number.

Precautions

Ensure that the port number configured on the device is the same as that used by the Portal server.

Example

Set the port number that a Portal server uses to receive packets from the device to 10000 in the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] port 10000
```

13.6.109 portal auth-network

Function

The **portal auth-network** command configures a source subnet for Portal authentication.

The **undo portal auth-network** command restores the default source subnet for Portal authentication.

By default, the source subnet for Portal authentication is 0.0.0.0/0, indicating that users in all subnets must pass Portal authentication.

Format

portal auth-network *network-address* { *mask-length* | *mask-address* }

undo portal auth-network { *network-address* { *mask-length* | *mask-address* } | **all** }

Parameters

Parameter	Description	Value
network-address	Specifies the IP address of the source subnet for Portal authentication.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 1 to 32.
mask-address	Specifies the mask of the source subnet for Portal authentication.	The value is in dotted decimal notation.
all	Deletes all Portal authentication subnets.	-

Views

GE interface view, MultiGE interface viewXGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk, interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source subnet for Portal authentication is configured, only user packets from the source subnet can trigger Portal authentication. If an unauthenticated user is not on the source subnet for Portal authentication, the device discards the user's packets that do not match Portal authentication free rules.

NOTE

The command cannot be run on Layer 2 interfaces.

The **portal auth-network** command takes effect only for Layer 3 Portal authentication. In Layer 2 authentication, users on all network segments must be authenticated.

Prerequisites

Before running this command on an interface, ensure that the Portal service template is bound to the interface.

Example

Set the source subnet for Portal authentication to 192.168.1.0/24 on VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] server-ip 10.1.1.1
[HUAWEI-web-auth-server-test] quit
```



```
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] web-auth-server test layer3
[HUAWEI-Vlanif10] portal auth-network 192.168.1.0 24
```

Set the source subnet for Portal authentication to 192.168.1.0/24 on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] server-ip 10.1.1.1
[HUAWEI-web-auth-server-test] quit
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] web-auth-server test layer3
[HUAWEI-GigabitEthernet0/0/1] portal auth-network 192.168.1.0 24
```

13.6.110 portal domain

Function

The **portal domain** specifies a forcible Portal authentication domain.

The **undo portal domain** command deletes a forcible Portal authentication domain.

By default, no forcible Portal authentication domain is specified.

Format

portal domain *domain-name*

undo portal domain

Parameters

Parameter	Description	Value
domain-name	Specifies the forcible Portal authentication domain.	The value is a string of 1 to 64 case-insensitive characters without any space, asterisk (*), question mark (?), or quotation mark (").

Views

GE interface view,MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

To flexibly deploy access policies for Portal authentication users, the administrator can run the **portal domain** command to configure a forcible Portal authentication domain.

After a forcible Portal authentication domain is configured on an interface, the device uses the specified authentication domain to authenticate, authorize, and charge Portal authentication users on the interface, ignoring the domain names carried in the user names. The administrator can specify different authentication domains for different interfaces as needed.

NOTE

The command cannot be run on Layer 2 interfaces.

Example

Set the forcible Portal authentication domain to **abc** on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] portal domain abc
```

Set the forcible Portal authentication domain to **abc** on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] portal domain abc
```

13.6.111 portal free-rule

Function

The **portal free-rule** command configures the Portal authentication-free rule for users.

The **undo portal free-rule** command restores the default configuration.

By default, no Portal authentication-free rule is configured.

Format

portal free-rule *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } [**tcp destination-port** *port* | **udp destination-port** *port*] | **any** } } | **source** { **any** | { **interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* } * } *

portal free-rule *rule-id* **source ip** *ip-address* **mask** { *mask-length* | *ip-mask* } [**mac** *mac-address*] [**interface** *interface-type interface-number*] **destination user-group** *group-name*

undo portal free-rule { *rule-id* | **all** }

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of the Portal authentication-free rule.	The value is an integer of which the range depends on product models.
destination	Specifies the destination network resources that the authentication-free users can access.	-
source	Specifies the source information of the authentication-free users.	-
any	Specifies any condition. When **any** is used together with different keywords, the effect of the command is different.	-
ip *ip-address*	Specifies the IP address in the rule. This parameter can specify the source or destination address depending on the keyword.	The value is in dotted decimal notation.
mask *mask-length*	Specifies the mask length of an IP address. This parameter can specify the source or destination address mask depending on the keyword.	The value is an integer that ranges from 1 to 32.
mask *ip-mask*	Specifies the IP address mask. This parameter can specify the source or destination address mask depending on the keyword.	The value is in dotted decimal notation.
tcp destination-port *port*	Specifies the TCP destination port number.	The value is an integer that ranges from 1 to 65535.
udp destination-port *port*	Specifies the UDP destination port number.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the source interface in the rule. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
vlan *vlan-id*	Specifies the VLAN ID of the source packet in the rule.	The value is an integer that ranges from 1 to 4094.
all	Specifies all rules.	-
mac *mac-address*	Specifies the MAC address of the Portal authentication user who is allowed to access destination network resources without authentication.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
user-group *group-name*	Allows Portal authentication users to access the network resources in the user group.	It is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user cannot access the network before being authenticated successfully. You can configure an authentication-free rule for specified users to access certain network resources without passing the Portal authentication. An authentication-free rule can be determined by parameters such as the IP address, MAC address, interface, and VLAN. An authentication-free rule can also be determined by ACL rules. The destination IP address that users can access without authentication can be specified in an authentication-free rule defined by either of the two methods. In addition, the destination domain name that users can access without authentication can be specified in an authentication-free rule defined by ACL.

For example, some authentication users who do not have an authentication account must first log in to the official website of a carrier and apply for a member account, or log in using the account of a third party such as Twitter or

Facebook. This requires that the users can access specified websites before successful authentication. The domain name of a website is easier to remember than the IP address; therefore, the authentication-free rule defined by ACL can be configured to enable the users to access the domain names of websites without authentication.

Precautions

- When multiple authentication-free rules are configured, the system matches the rules one by one.
- If the **vlan** parameter determines where users reside for an authentication-free rule, the Portal server must have been bound to the VLANIF interface of the VLAN using the **web-auth-server (interface view)** command; otherwise, the configured authentication-free rule does not take effect for users in the VLAN.
- If you specify both VLAN and interface when running the **portal free-rule** command, the interface must belong to the VLAN; otherwise, the configuration is invalid.
- If you specify the destination port number in an authentication-free rule, fragmented packets cannot match the rule and cannot be forwarded.
- You can only add or delete rules, but cannot modify the created rules. To modify a rule with a certain *rule-id*, run the **undo portal free-rule** command to delete the rule and re-configure it.
- To allow Portal authentication users to access the network resources in the user group, pay attention to the following points:
  - The user group has been created before it is referenced by the Portal authentication-free rule.
  - The Portal authentication-free rule takes effect only after the referenced user group is enabled.
  - A user can only join one user group. If multiple rules are configured, the rule with the smallest *rule-id* has the highest priority.
  - If multiple rules are applied to a user, the Portal authentication-free rule referencing the user group has the highest priority.
  - The rule of the user group can only contain whitelists. That is, the deny action cannot be used.
  - After configuring authorization for a user using the **destination user-group** *group-name* command, you cannot configure authorization in other modes for the user.

Example

Enable all Portal users to access the network 10.1.1.1/24 without authentication.

```
<HUAWEI> system-view
[HUAWEI] portal free-rule 1 destination ip 10.1.1.1 mask 24 source ip any
```

Add the devices on network segment 10.2.100.0/24 to the user group **static-user**, and allow the devices to access resources on this network segment without authentication.

```
<HUAWEI> system-view
[HUAWEI] acl number 3100
[HUAWEI-acl-adv-3100] rule 5 permit ip source 10.2.100.0 255.255.255.0
[HUAWEI-acl-adv-3100] quit
```



```
[HUAWEI] user-group static-user
[HUAWEI-user-group-static-user] acl-id 3100
[HUAWEI-user-group-static-user] quit
[HUAWEI] user-group static-user enable
[HUAWEI] portal free-rule 0 source ip 10.2.100.0 mask 24 destination user-group static-user
```

13.6.112 portal https-redirect blacklist

Function

The **portal https-redirect blacklist** command adds an address to the HTTPS redirection blacklist. After an address is added to the HTTPS redirection blacklist, HTTPS redirection is not performed for HTTPS access to this address of Portal users.

The **undo portal https-redirect blacklist** command removes an address from the HTTPS redirection blacklist.

By default, no address is added to the HTTPS redirection blacklist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist ip *start-ip-address* [*end-ip-address*]

portal https-redirect blacklist ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]

undo portal https-redirect blacklist ip { *start-ip-address* [*end-ip-address*] | **all** }

undo portal https-redirect blacklist ipv6 { *start-ipv6-address* [**to** *end-ipv6-address*] | **all** }

Parameters

Parameter	Description	Value
ip *start-ip-address* [*end-ip-address*]	Specifies an IPv4 address or an IPv4 address range: • *start-ip-address* specifies the start IPv4 address. • *end-ip-address* specifies the end IPv4 address.	-

Parameter	Description	Value
ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]	Specifies an IPv6 address or an IPv6 address range: ● *start-ipv6-address* specifies the start IPv6 address. ● *end-ipv6-address* specifies the end IPv6 address.	-
all	Removes all IPv4 addresses or IPv6 addresses from the HTTPS redirection blacklist.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before users pass Portal authentication, HTTPS access to a website other than the Portal server triggers HTTPS redirection by default. To disable HTTPS redirection for HTTPS access to a specified address, run the **portal https-redirect blacklist** command to add this address to the HTTPS redirection blacklist.

Precautions

If an address has been added to the HTTPS redirection whitelist using the **portal https-redirect whitelist** command, this address cannot be added to the HTTPS redirection blacklist.

If an address (except the address of the Portal server) is not in the HTTPS redirection blacklist, HTTPS access to this address will always trigger HTTPS redirection before users pass Portal authentication.

Example

Add 10.1.1.1 to the HTTPS redirection blacklist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist ip 10.1.1.1
```

Add FC00::1 to the HTTPS redirection blacklist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist ipv6 FC00::1
```


13.6.113 portal https-redirect blacklist aging-time

Function

The **portal https-redirect blacklist aging-time** command configures the aging time of addresses in the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist aging-time** command restores the default aging time of addresses in the HTTPS redirection blacklist.

By default, the aging time of addresses in the HTTPS redirection blacklist is 259200 seconds, that is, 72 hours.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist aging-time *aging-time*

undo portal https-redirect blacklist aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of addresses in the HTTPS redirection blacklist.	The value is an integer in the range from 30 to 4294967295, in seconds. The default value is 259200 seconds, that is, 72 hours.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After an address (except the address of the Portal server) is added to the HTTPS redirection blacklist, HTTPS access from Portal users to this address does not trigger HTTPS redirection. By default, the aging time of addresses in the HTTPS redirection blacklist is 259200 seconds. When the aging time expires, this address will be removed from the blacklist. You can use the **portal https-redirect blacklist**

aging-time command to adjust the aging time of addresses in the HTTPS redirection blacklist.

Example

Configure the aging time of addresses in the HTTPS redirection blacklist to 86400 seconds, that is, 24 hours.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist aging-time 86400
```

13.6.114 portal https-redirect blacklist packet-rate

Function

The **portal https-redirect blacklist packet-rate** command configures the maximum rate at which a Portal user accesses an address through HTTPS. If the user access rate reaches the maximum, the switch adds the destination address to the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist packet-rate** command restores the default maximum rate at which a Portal user accesses an address through HTTPS.

By default, the maximum rate at which a Portal user accesses an address through HTTPS is 40 times per minute.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist packet-rate *packet-rate*

undo portal https-redirect blacklist packet-rate

Parameters

Parameter	Description	Value
packet-rate	Specifies the maximum rate at which a Portal user accesses an address through HTTPS.	The value is an integer in the range from 5 to 600, in times per minutes. The default value is 40.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the switch redirects the HTTP or HTTPS requests sent from clients to the Portal login page. When the rate of packets sent from a Portal user for accessing an address through HTTPS reaches the maximum rate specified by the **portal https-redirect blacklist packet-rate** command, the switch adds the destination address to the HTTPS redirection blacklist. This prevents repeated HTTPS redirection caused by frequent access from malicious users to an address, and therefore saves resources of the switch.

Prerequisites

The function of inserting a JavaScript file during Portal redirection has been enabled using the **portal redirect js enable** command.

Precautions

This command takes effect only for the HTTPS protocol.

This command takes effect for both IPv4 and IPv6 addresses.

Example

Set the maximum rate at which a Portal user accesses an address through HTTPS to 30 times per minute.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist packet-rate 30
```

13.6.115 portal https-redirect blacklist retry-times interval

Function

The **portal https-redirect blacklist retry-times interval** command configures the maximum number of times and the detection period. Within the detection period, if the number of times an address is added to the provisional HTTPS redirection blacklist reaches the maximum, the address is added to the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist retry-times interval** command restores the default maximum number of times and the default detection period.

By default, the maximum number of times is 10 and the detection period is 3 minutes.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist retry-times *retry-times* **interval** *interval*

undo portal https-redirect blacklist retry-times interval

Parameters

Parameter	Description	Value
retry-times	Specifies the maximum number of times.	The value is an integer in the range from 1 to 600. The default value is 10.
interval	Specifies the detection period.	The value is an integer in the range from 1 to 600, in minutes. The default value is 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the switch redirects the HTTP or HTTPS requests sent from clients to the Portal login page. When the function of inserting a JavaScript file during Portal redirection is enabled on the switch using the **portal redirect js enable** command, the HTTP or HTTPS response packets sent from the switch to clients carry the JavaScript file.

- The clients can be redirected to the Portal login page only after they correctly parse the JavaScript file.
- If a client fails to parse the JavaScript file, the switch adds the destination address to the provisional HTTPS redirection blacklist. HTTP and HTTPS redirection can still be triggered for addresses in the provisional HTTPS redirection blacklist.

The detection period specified in the **portal https-redirect blacklist retry-times interval** command starts from the time when an address is added to the provisional HTTPS redirection blacklist. If the number of times an address is added to the provisional HTTPS redirection blacklist reaches the maximum within the detection period, this address is added to the HTTPS redirection blacklist.

Precautions

This command takes effect only for the HTTPS protocol.

This command takes effect for both IPv4 and IPv6 addresses.

Example

Set the maximum number of times to 15 and the detection period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist retry-times 15 interval 5
```

13.6.116 portal https-redirect whitelist

Function

The **portal https-redirect whitelist** command adds an address to the HTTPS redirection whitelist.

The **undo portal https-redirect whitelist** command removes an address from the HTTPS redirection whitelist.

By default, no address is added to the HTTPS redirection whitelist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect whitelist ip *start-ip-address* [*end-ip-address*]

portal https-redirect whitelist ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]

undo portal https-redirect whitelist ip { *start-ip-address* [*end-ip-address*] | **all** }

undo portal https-redirect whitelist ipv6 { *start-ipv6-address* [**to** *end-ipv6-address*] | **all** }

Parameters

Parameter	Description	Value
ip *start-ip-address* [*end-ip-address*]	Specifies an IPv4 address or an IPv4 address range: • *start-ip-address* specifies the start IPv4 address. • *end-ip-address* specifies the end IPv4 address.	-

Parameter	Description	Value
ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]	Specifies an IPv6 address or an IPv6 address range: ● *start-ipv6-address* specifies the start IPv6 address. ● *end-ipv6-address* specifies the end IPv6 address.	-
all	Removes all IPv4 addresses or IPv6 addresses from the HTTPS redirection whitelist.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before users pass Portal authentication, HTTPS access to a website other than the Portal server triggers HTTPS redirection by default. If an address is added to the HTTPS redirection blacklist by mistake, HTTPS access to this address will not trigger HTTPS redirection. To ensure that HTTPS redirection is performed for HTTPS access to specified addresses, use the **portal https-redirect whitelist** command to add these addresses to the HTTPS redirection whitelist.

Configuration Impact

If an address has been added to the HTTPS redirection whitelist, this address cannot be added to the HTTPS redirection blacklist using the **portal https-redirect blacklist** command.

Precautions

If an address in the HTTPS redirection blacklist is added to the HTTPS redirection whitelist, the switch removes the address from the HTTPS redirection blacklist.

If an address (except the address of the Portal server) is not in the HTTPS redirection blacklist, HTTPS access to this address will always trigger HTTPS redirection before users pass Portal authentication.

Example

Add 10.1.2.1 to the HTTPS redirection whitelist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect whitelist ip 10.1.2.1
```

Add FC00::2 to the HTTPS redirection whitelist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect whitelist ipv6 FC00::2
```

13.6.117 portal logout different-server enable

Function

The **portal logout different-server enable** command configures a device to process user logout requests sent by a Portal server other than the one from which users log in.

The **undo portal logout different-server enable** command restores the default configuration.

By default, a device does not process user logout requests sent by Portal servers other than the one from which users log in.

Format

portal logout different-server enable

undo portal logout different-server enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario where Portal server load balancing is configured, by default, a device does not process user logout requests sent by Portal servers other than the one from which users log in and responds ACK messages only to the Portal server from which users log in. Users in arrears then can still stay online. To prevent this problem, run **portal logout different-server enable** command to configure the device to process user logout requests sent by a Portal server other than the one from which users log in. Upon receipt of a user logout request from such a Portal server, the device starts a user logout process. After completing the logout event,

the device responds an ACK message to the Portal server, thereby ensuring that the user logs out properly.

Precautions

The user logout requests that a device can process must be sent by Portal servers bound to an access interface. These servers include all the Portal servers configured in the master and backup Portal server templates bound to the interface.

Example

Enable a device to process user logout requests a Portal server other than the one from which users log in.

```
<HUAWEI> system-view
[HUAWEI] portal logout different-server enable
```

13.6.118 portal logout resend timeout

Function

The **portal logout resend timeout** command configures the re-transmission times and interval for the Portal authentication user logout packet.

The **undo portal logout resend timeout** command restores the default setting.

By default, the Portal authentication user logout packet can be re-transmitted three times within five seconds.

Format

portal logout resend *times* **timeout** *period*

undo portal logout { **resend** | **timeout** } *

Parameters

Parameter	Description	Value
times	Specifies the number of re-transmission times for the Portal authentication user logout packet.	The value is an integer that ranges from 0 to 15. The value 0 indicates that the re-transmission function is disabled.
period	Specifies the re-transmission interval of the Portal authentication user logout packet.	The value is an integer that ranges from 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After disconnecting a Portal authentication user, the device sends a user logout packet (NTF-LOGOUT) to instruct the Portal server to delete the user information. If the network between the device and Portal server is not stable or packets are lost, the Portal server may fail to receive the user logout packet from the device after the Portal authentication user is disconnected. In this case, the user is displayed as disconnected on the device but still as online on the Portal server. To enable the Portal server to receive the user logout packet and ensure that the online user information on the Portal server is correct, the administrator can enable the user logout packet re-transmission function on the device and configure the re-transmission times and interval.

Example

Configure the re-transmission times to 5 and interval to 10 seconds for the Portal authentication user logout packet.

```
<HUAWEI> system-view
[HUAWEI] portal logout resend 5 timeout 10
```

13.6.119 portal max-user

Function

The **portal max-user** command sets the maximum number of concurrent Portal authentication users allowed to access the device.

The **undo portal max-user** command restores the default maximum number of concurrent Portal authentication users.

By default, the number of Portal authentication users is the maximum number of Portal authentication users supported by the device.

Format

portal max-user *user-number*

undo portal max-user

Parameters

Parameter	Description	Value
user-number	Specifies the maximum number of concurrent Portal users.	The value is an integer that varies depending on product models.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **portal max-user** command to set the maximum number of concurrent Portal authentication users.

Example

Set the maximum number of concurrent Portal authentication users to 25.

```
<HUAWEI> system-view
[HUAWEI] portal max-user 25
```

13.6.120 portal quiet-period

Function

The **portal quiet-period** command enables the quiet timer for Portal authentication.

The **undo portal quiet-period** command disables the quiet timer of Portal authentication.

By default, the quiet timer for Portal authentication is enabled.

Format

portal quiet-period

undo portal quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer for Portal authentication. If the number of Portal authentication failures exceeds the

value specified by the **portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. During the quiet period, the device discards Portal authentication requests from the user. This prevents the impact of frequent authentications on the system.

The quiet period for Portal authentication can be set using the **portal timer quiet-period** command. After the quiet period is reached, the device re-authenticates the user.

Example

Enable the quiet timer for Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal quiet-period
```

13.6.121 portal quiet-times

Function

The **portal quiet-times** command sets the maximum number of authentication failures within 60s before a Portal authentication user is kept in quiet state.

The **undo portal quiet-times** command restores the default maximum number of authentication failures within 60s before a Portal authentication user enters the quiet state.

By default, the device allows a maximum of ten authentication failures within 60s before a Portal authentication user enters the quiet state.

Format

portal quiet-times *fail-times*

undo portal quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a Portal authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer, if the number of Portal authentication failures exceeds the value specified by the **portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. This prevents the impact of frequent authentications on the system.

Example

Set the maximum number of Portal authentication failures within 60 seconds to 4.

```
<HUAWEI> system-view
[HUAWEI] portal quiet-times 4
```

13.6.122 portal redirect js enable

Function

The **portal redirect js enable** command enables the function of inserting a JavaScript file during Portal redirection.

The **undo portal redirect js enable** command disables the function of inserting a JavaScript file during Portal redirection.

By default, the function of inserting a JavaScript file during Portal redirection is disabled.

Format

portal redirect js enable

undo portal redirect js enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the device redirects the HTTP or HTTPS requests sent from clients to the Portal server. To prevent heavy burdens on the server caused by a large number of HTTP or HTTPS requests sent from the clients and to ensure proper display of the Portal login page, enable the function of

inserting a JavaScript file during Portal redirection. After this function is enabled, the HTTP or HTTPS response packets sent from the server carry a JavaScript file. The client browser parses the JavaScript file for redirection, and then performs Portal authentication.

Precautions

The client browser must support and enable the JavaScript function.

Example

Enable the function of inserting a JavaScript file during Portal direction.

```
<HUAWEI> system-view
[HUAWEI] portal redirect js enable
```

13.6.123 portal timer offline-detect

Function

The **portal timer offline-detect** command sets the Portal user offline detection interval.

The **undo portal timer offline-detect** command restores the default Portal user offline detection interval.

By default, the Portal user offline detection interval is 300 seconds.

Format

portal timer offline-detect *time-length*

undo portal timer offline-detect

Parameters

Parameter	Description	Value
time-length	Specifies the Portal user offline detection interval.	The value is 0 or an integer that ranges from 30 to 7200, in seconds. The default value is 300. The value 0 indicates that offline detection is not performed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a Portal user goes offline due to power failure or network interruption, the device and Portal server may still store the user information, which causes incorrect accounting. Additionally, a limit number of users can access the device. If a user goes offline improperly but the device still stores user information, other users cannot access the network.

After the Portal user offline detection interval is set, if the user does not respond within the interval, the device considers the Portal user offline. The device and Portal server then delete the user information and release resources to ensure an efficient resource use.

Precautions

This command only applies to Layer 2 Portal authentication. When the configuration is changed, the new configuration takes effect only for new access users.

The heartbeat detection function of the authentication server can be used to ensure the normal online status of PC users for whom Layer 3 Portal authentication is used. If the authentication server detects that a user goes offline, it instructs the device to disconnect the user.

If the number of offline detection packets (ARP packets) exceeds the default CAR value, the detection fails and the users are logged out. (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.) To resolve the problem, the following methods are recommended:

- Increase the detection interval based on the number of users. The default detection interval is recommended when there are less than 8000 users; the detection interval should be no less than 600 seconds when there are more than 8000 users.
- Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

If user traffic (such as service packets) passes through the device within the Portal user offline detection period, the device does not consider the user offline even if the user does not respond.

Example

Set the Portal user offline detection interval to 400s.

```
<HUAWEI> system-view
[HUAWEI] portal timer offline-detect 400
```

13.6.124 portal timer quiet-period

Function

The **portal timer quiet-period** command sets the quiet period for Portal authentication.

The **undo portal timer quiet-period** command restores the default quiet period for Portal authentication.

By default, the quiet period for Portal authentication is 60s.

Format

portal timer quiet-period *quiet-period-value*

undo portal timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-value	Specifies the quiet period for Portal authentication.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer, run the **portal timer quiet-period** command to set the quiet period for Portal authentication. If a Portal authentication user is kept in quiet state, the device discards Portal authentication requests from the user during the quiet period.

Example

Set the quiet period to 2000s.

```
<HUAWEI> system-view
[HUAWEI] portal timer quiet-period 2000
```

13.6.125 portal url-encode enable

Function

The **portal url-encode enable** command enables URL encoding and decoding.

The **undo portal url-encode enable** command disables URL encoding and decoding.

By default, URL encoding and decoding are enabled.

Format

portal url-encode enable

undo portal url-encode enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve web application security, data from untrustworthy sources must be encoded before being sent to clients. URL encoding is most commonly used in web applications. To enable URL encoding and decoding, run the **portal url-encode enable** command. Some special characters in redirect URLs are then converted to secure formats, preventing clients from mistaking them for syntax signs or instructions and unexpectedly modifying the original syntax. In this way, cross-site scripting attacks and injection attacks are prevented.

Precautions

After the URL encoding and decoding function is enabled, some servers may not support the escape characters converted from special characters in redirect URLs. Therefore, check whether servers support the escape characters before configuring special characters in redirect URLs.

Example

Enable URL encoding and decoding.

```
<HUAWEI> system-view
[HUAWEI] portal url-encode enable
```

13.6.126 portal user-alarm percentage

Function

The **portal user-alarm percentage** command sets alarm thresholds for the Portal authentication user count percentage.

The **undo portal user-alarm percentage** command restores the default alarm thresholds for the Portal authentication user count percentage.

By default, the lower alarm threshold for the Portal authentication user count percentage is 50, and the upper alarm threshold for the Portal authentication user count percentage is 100.

Format

portal user-alarm percentage *percent-lower-value percent-upper-value*

undo portal user-alarm percentage

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **portal max-user** command to set the maximum number of online Portal authentication users allowed on a device, you can run the **portal user-alarm percentage** command to set alarm thresholds for the Portal authentication user count percentage.

When the percentage of online Portal authentication users against the maximum number of users allowed by the device exceeds the upper alarm threshold, the device generates an alarm. When the percentage of online Portal authentication users against the maximum number of users allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm.

If the configured upper alarm threshold for the Portal authentication user count percentage is 100, the device generates an alarm when the number of online users reaches the maximum number of users allowed by the device.

Example

Set the lower alarm threshold for the Portal authentication user count percentage to 30, and the upper alarm threshold for the Portal authentication user count percentage to 80.

```
<HUAWEI> system-view
[HUAWEI] portal user-alarm percentage 30 80
```


13.6.127 portal web-authen-server

Function

The **portal web-authen-server** command enables the Portal interconnection function of the HTTP or HTTPS protocol.

The **undo portal web-authen-server** command disables the Portal interconnection function of the HTTP or HTTPS protocol.

By default, the Portal interconnection function of the HTTP or HTTPS protocol is disabled.

Format

portal web-authen-server { **http** | **https ssl-policy** *policy-name* } [**port** *port-number*]

undo portal web-authen-server [**port**]

Parameters

Parameter	Description	Value
http	Sets the HTTP protocol for Portal authentication. **NOTE** The HTTP protocol poses security risks. The HTTPS protocol is recommended.	-
https	Sets the HTTPS protocol for Portal authentication.	-
ssl-policy *policy-name*	Specifies the name of an SSL policy.	The value must be the name of an existing SSL policy.
port *port-number*	Specifies a port number.	The value is an integer that ranges from 1025 to 55535. The default HTTP port number is 8000 and the default HTTPS port number is 8443.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is connected to the Portal server that only supports the HTTP or HTTPS protocol, you need to run the **portal web-authen-server** command on the device to enable the Portal interconnection function of the HTTP or HTTPS protocol.

Follow-up Procedure

Run the **protocol** command to set the protocol used in Portal authentication to HTTP or HTTPS.

Precautions

Modifying the **port** parameter causes the pre-connected user to go offline.

Example

Enable the Portal interconnection function of the HTTPS protocol.

```
<HUAWEI> system-view
[HUAWEI] ssl policy huawei
[HUAWEI-ssl-policy-huawei] quit
[HUAWEI] portal web-authen-server https ssl-policy huawei port 8443
```

13.6.128 protocol (Portal server template view)

Function

The **protocol** command configures the protocol used in Portal authentication.

The **undo protocol** command restores the default configuration.

By default, the Portal protocol is used in Portal authentication.

Format

protocol { **http** [**password-encrypt** { **none** | **uam** }] | **portal** }

undo protocol

Parameters

Parameter	Description	Value
http	Sets the protocol used in Portal authentication to HTTP or HTTPS.	-

Parameter	Description	Value
password-encrypt { **none** | **uam** }	Specifies the password encoding mode. • **none**: The password is not encoded. • **uam**: The password is encoded using ASCII characters.	-
portal	Sets the protocol used in Portal authentication to Portal.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

In Portal authentication, the device can use the following protocols to communicate with the Portal server. You can set the protocol according to the protocol supported by the Portal server.

- Portal protocol
- HTTP or HTTPS protocol

Example

Set the protocol used in Portal authentication to HTTP or HTTPS.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] protocol http password-encrypt uam
```

13.6.129 remark

Function

The **remark** command configures the user group priority.

The **undo remark** command cancels the user group priority configuration.

By default, no user group priority is configured.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

remark { **8021p** *8021p-value* | **dscp** *dscp-value* } *

undo remark { **8021p** *8021p-value* | **dscp** *dscp-value* } *

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the priority for processing Layer 2 Ethernet packets.	The value is an integer that ranges from 0 to 7.
dscp *dscp-value*	Specifies the priority for processing IP packets.	The value is an integer that ranges from 0 to 63.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the user group priority is configured, users in the user group inherit the priority. That is, different user packets have different priorities. In this way, the administrator can manage different types of users more flexibly.

Precautions

When the **remark** and **voice-vlan remark** commands are used together to modify the user packet priority, if the services conflict:

- For S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the priority configured using the **remark** command takes effect.
- For S6720-EI, S6720S-EI, the priority configured using the **voice-vlan remark** command takes effect.

Example

Set the priority for processing IP packets to 3 in the user group **abc**.

```
<HUAWEI> system-view
[HUAWEI] user-group abc
[HUAWEI-user-group-abc] remark dscp 3
```

13.6.130 reset aaa statistics access-type-authenreq

Function

The **reset aaa statistics access-type-authenreq** command clears the number of requesting for MAC, Portal, or 802.1X authentication.

Format

reset aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, and 802.1X authentications.

To clear the number of requesting for MAC, Portal, or 802.1X authentication, run the **reset aaa statistics access-type-authenreq** command.

Example

Clear the number of requesting for MAC, Portal, or 802.1X authentication.

```
<HUAWEI> reset aaa statistics access-type-authenreq
```

13.6.131 reset access-user dot1x-identity statistics

Function

The **reset access-user dot1x-identity statistics** command clears statistics about Identity packets for 802.1X authentication on a switch.

Format

reset access-user dot1x-identity statistics

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To display statistics about Identity packets for 802.1X authentication on a switch within a specified period of time, run the **reset access-user dot1x-identity statistics** command to clear the existing statistics first, and then run the **display access-user dot1x-identity statistics** command to display the new statistics.

Example

Clear statistics about Identity packets for 802.1X authentication on the switch.

```
<HUAWEI> system-view
[HUAWEI] reset access-user dot1x-identity statistics
```

13.6.132 reset access-user traffic-statistics

Function

The **reset access-user traffic-statistics** command clears statistics on traffic of online users in a user group.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

reset access-user traffic-statistics { **user-id** *begin-id* [*end-id*] | **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance*] }

Parameters

Parameter	Description	Value
user-id *begin-id* [*end-id*]	Specifies IDs of online users. • *begin-id* specifies the start ID of online users. • *end-id* specifies the end ID of online users. The value of *end-id* must be equal to or greater than that of *begin-id*. To view IDs of online users, run the **display access-user** command.	The value is an integer that varies depending on the product model.

Parameter	Description	Value
mac-address *mac-address*	Specifies the MAC address of an online user.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
ip-address *ip-address*	Specifies the IP address of an online user.	The value is in dotted decimal notation.
vpn-instance *vpn-instance*	Specifies the VPN instance that an online user belongs to.	The value must be an existing VPN instance name.

Views

User view

Default Level

3: Management level

Usage Guidelines

After traffic control is configured for users in a user group using the **car** command, the device collects statistics on traffic of each user in the user group. You can run the **reset access-user traffic-statistics** command to clear statistics on traffic of online users in a user group.

NOTE

After you run the **reset access-user traffic-statistics** command to clear traffic statistics, the cleared user traffic statistics are not included in the accounting packets sent by the device to the accounting server.

Example

Clear statistics on traffic of the user with the IP address as 10.1.1.1.

```
<HUAWEI> reset access-user traffic-statistics ip-address 10.1.1.1
```

13.6.133 reset dot1x statistics

Function

The **reset dot1x statistics** command clears 802.1X authentication statistics.

Format

reset dot1x statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears 802.1X authentication statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, 802.1X authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The 802.1X authentication statistics contain the number of times that the authentication succeeded and failed on an interface and the number of sent and received packets.

The **reset dot1x statistics** command is used in the following scenarios:

- Redeploy services. After the statistics are cleared, collect the 802.1X authentication statistics again, and run the **display dot1x** command to check whether the authentication function works properly and whether packets are correctly sent and received.
- Rectify a fault. After the fault is rectified, run the **reset dot1x statistics** command to clear the statistics, collect the statistics on 802.1X authentication again, and then run the **display dot1x** command to verify the authentication result and check whether packets are correctly sent and received. If the authentication is successful and packets are correctly sent and received, the fault is rectified.

Example

Clear 802.1X authentication statistics on GE0/0/1.

```
<HUAWEI> reset dot1x statistics interface gigabitethernet 0/0/1
```


13.6.134 reset mac-authen statistics

Function

The **reset mac-authen statistics** command clears MAC address authentication statistics.

Format

reset mac-authen statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears MAC address authentication statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, MAC address authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset mac-authen statistics** command is used in the following scenarios:

- Re-deploy services. After the statistics are cleared, collect the MAC address authentication statistics again, and run the **display mac-authen** command to check whether the authentication function is normal.
- Rectify a fault. After the fault is rectified, run the **reset mac-authen statistics** command to clear statistics, collect MAC address authentication statistics again, and run the **display mac-authen** command to check the authentication result. If the authentication is successful, the fault is rectified.

Example

Clear MAC address authentication statistics on GE0/0/1.

```
<HUAWEI> reset mac-authen statistics interface gigabitethernet 0/0/1
```

13.6.135 server-detect

Function

The **server-detect** command enables the Portal server detection function.

The **undo server-detect** command disables the Portal server detection function.

By default, the Portal server detection function is disabled.

Format

server-detect [**interval** *interval-period* | **max-times** *times* | **critical-num** *critical-num* | **action** { **log** | **trap** | **permit-all** } *] *

undo server-detect [**interval** | **max-times** | **critical-num** | **action** { **log** | **trap** | **permit-all** } *]

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the detection interval of the Portal server.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 60.
max-times *times*	Specifies the maximum number of times that the detection fails.	The value is an integer that ranges from 1 to 255. The default value is 3.
critical-num *critical-num*	Specifies the minimum number of Portal servers in Up state.	The value is an integer that ranges from 0 to 128. The default value is 0. The default value is recommended.
action	Specifies the action to be taken after the number of detection failures exceeds the maximum.	-

Parameter	Description	Value
log	Indicates that the device sends a log after the number of detection failures exceeds the maximum.	-
trap	Indicates that the device sends a trap after the number of detection failures exceeds the maximum.	-
permit-all	Cancels Portal authentication on an interface after the number of detection failures exceeds the maximum.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

If the communication is interrupted because the network between the device and Portal server is faulty or the Portal server is faulty, new Portal authentication users cannot go online. This brings great inconvenience to users.

After the Portal server detection function is enabled in the Portal server template, the device detects all Portal servers configured in the Portal server template. If the number of times that the device fails to detect a Portal server exceeds the upper limit, the status of the Portal server is changed from Up to Down. If the number of Portal servers in Up state is less than or equal to the minimum number (specified by the **critical-num** parameter), the device performs the corresponding operation to allow the administrator to obtain the real-time Portal server status or ensure that the users have certain network access rights.

NOTE

The detection interval of the Portal server multiplied by the maximum number of detection failures cannot be less than the keepalive heartbeat interval of the Portal server. It is recommended that the configured detection interval of the Portal server be greater than the keepalive heartbeat interval of the Portal server.

If the Portal server does not support detection, you do not need to configure this command.

Example

Enable the Portal server detection function in the Portal server template abc. Configure the detection interval to 100 seconds, the maximum number of detection failures to 5. Configure the device to send log information when the number of detection failures exceeds the upper limit.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] server-detect interval 100 max-times 5 action log
```

13.6.136 server-detect type

Function

The **server-detect type** command configures the mode in which a device detects Portal server status.

The **undo server-detect type** command restores the default Portal server detection mode.

By default, the Portal-based Portal server detection mode is configured.

Format

server-detect type { **portal** | **http** }

undo server-detect type

Parameters

Parameter	Description	Value
portal	Specifies the Portal-based Portal server detection mode.	-
http	Specifies the HTTP-based Portal server detection mode.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Precautions

In Portal-based Portal server detection mode, the Portal server periodically (the time is determined by the server) sends heartbeat packets to the access device,

which then determines the server reachability based on the heartbeat packets. If the access device receives Portal heartbeat packets or other authentication packets from the Portal server within the detection interval (configured using **server-detect interval** *interval-period*) and the packets are verified to be correct, the detection is successful. Otherwise, the detection fails. When the number of consecutive detection failures reaches the maximum number specified by the **server-detect max-times** *times* command, the access device changes the status of the Portal server from Up to Down.

In HTTP-based Portal server detection mode, the access device periodically sends HTTP packets to the Portal server and expects a response packet from the Portal server. If the access device receives a response packet within the specified detection interval (configured using **server-detect interval** *interval-period*), the detection is successful. Otherwise, the detection fails. When the number of consecutive detection failures reaches the maximum number specified by the **server-detect max-times** *times* command, the access device changes the status of the Portal server from Up to Down.

In Portal-based Portal server detection mode, the Portal server must use the Portal protocol and support sending Portal heartbeat packets. If the Portal server does not meet these requirements, you can configure the HTTP-based detection mode. In this way, if the device detects that the Portal server is Down, the device grants new users the corresponding network access rights.

Precautions

HTTP-based Portal server detection applies to both wireless access scenarios and wired access scenarios using MAC+Portal authentication.

Example

Configure the device to detect Portal server status using HTTP.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] server-detect type http
```

13.6.137 server-ip (Portal server template view)

Function

The **server-ip** command configures an IP address for a Portal server.

The **undo server-ip** command deletes an IP address for a Portal server.

By default, no IP address is configured for a Portal server.

Format

server-ip *server-ip-address* &<1-10>

server-ip ipv6 *server-ipv6-address* &<1-3>

undo server-ip { *server-ip-address* **ipv6** *server-ipv6-address* | **all** }

NOTE

The **ipv6** *server-ipv6-address* parameter is only supported by the following models:

S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S500, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720-EI, S6720S-EI

Parameters

Parameter	Description	Value
server-ip-address	Specifies an IPv4 address of a Portal server.	The value is in dotted decimal notation.
ipv6 *server-ipv6-address*	Specifies an IPv6 address of a Portal server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
all	Deletes all IP addresses of a Portal server.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server template on the device using the **web-auth-server (system view)** command, configure parameters for the template.

Run the **server-ip** command to configure an IP address for the Portal server in the Portal server template view. When receiving a Portal authentication request packet from a user, the device sends a response packet to the Portal server with the configured IP address.

Precautions

- After the IP address corresponding to a Portal server is configured in the Portal server template, users are allowed to access the IP address.
- When a Portal server template is bound to an interface, server IP addresses can be added, but cannot be deleted. If multiple IP addresses are configured for a Portal server in the Portal server template, you are advised to run the **url (Portal server template view)** command to configure a URL for the Portal server. If no URL is configured, the device uses the first IP address as the URL by default, and the other IP addresses do not take effect.

- When you run the **server-ip** command to specify IPv6 addresses, you must also specify IPv4 addresses. This is because the device does not support IPv6 Portal protocol exchange.

Example

Set the Portal server IP address in the Portal server template **test** to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server huawei
[HUAWEI-web-auth-server-huawei] server-ip 10.10.10.1
```

13.6.138 shared-key (Portal server template view)

Function

The **shared-key** command configures the shared key that the device uses to exchange information with a Portal server.

The **undo shared-key** command restores the default setting.

By default, no shared key that the device uses to exchange information with a Portal server is configured.

Format

shared-key cipher *key-string*

undo shared-key

Parameters

Parameter	Description	Value
cipher	Displays a shared key in cipher text.	-
key-string	Specifies the shared key.	The value is a string of case-sensitive characters without spaces. It can be a string of 20 to 392 characters in cipher text, or a string of 1 to 255 characters in plain text.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a shared key is configured using the **shared-key** command, the Portal packet exchanged between the device and Portal server carries an authenticator generated according to the shared key, and the authenticator is used to check whether the Portal packet at the receiver is correct. This effectively improves the information exchange security.

Precautions

To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 16 characters.

Example

Configure the shared key in the Portal server template **test** to YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] shared-key cipher YsHsjx_202206
```

13.6.139 source-ip (Portal server template view)

Function

The **source-ip** command configures the source IP address for the device to communicate with a Portal server.

The **undo source-ip** command restores the default setting.

By default, no source IP address is configured for the device to communicate with a Portal server.

Format

source-ip *ip-address*

undo source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for communication with a Portal server.	The value is in dotted decimal notation.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure normal communication between the device and Portal server, run the **source-ip** command to configure a source IP address on the device.

If the device is configured with a loopback IP address and a common IP address, the device can communicate with the Portal server only when the loopback IP address and common IP address are the same. The **source-ip** command configures a source IP address on the device in the **web-auth-server** view to allow communication between the device and a Portal server.

Precautions

Ensure that the configured source IP address is the device IP address. The source IP address cannot be all 0s, 255.255.255.255, class D address, class E address, or loopback address.

Example

Set the source IP address for communication between the device and a Portal server to 192.168.1.100 in the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] source-ip 192.168.1.100
```

13.6.140 static-user

Function

The **static-user** command configures a static user.

The **undo static-user** command deletes the configured static user.

By default, no static user is configured.

Format

static-user *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*] [**domain-name** *domain-name* | **interface** *interface-type interface-number* [**detect**] | **mac-address** *mac-address* | **vlan** *vlan-id* | **keep-online**] *

undo static-user *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
start-ip-address [*end-ip-address*]	Specifies the IP address range that a static user belongs to. If *end-ip-address* is not specified, a static user is specified by *start-ip-address*.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that a static user belongs to.	The value must be an existing VPN instance name.
domain-name *domain-name*	Specifies the domain that a static user belongs to.	The value must be an existing domain name.
interface *interface-type interface-number*	Specifies the interface connected to a static user. ● *interface-type* specifies the interface type. **NOTE** A management interface cannot be configured as the interface to which a static user belongs. ● *interface-number* specifies the interface number.	-
detect	Permits the device to send ARP packets to trigger Portal authentication for static users in offline state.	-
mac-address *mac-address*	Specifies the MAC address of a static user.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
vlan *vlan-id*	Specifies the ID of a VLAN that a static user belongs to.	The value is an integer that ranges from 1 to 4094.
keep-online	Keeps a static user online, with offline detection not performed.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In network deployment, static IP addresses are assigned to dumb terminals such as printers and servers. These users can be configured as static users for flexible authentication.

After static users are configured, the device can use static user information such as their IP addresses as the user names to authenticate the users only when Portal authentication is enabled on the interfaces connected to the static users.

Precautions

When the interface (**interface** *interface-type interface-number*) mapping static users is specified, the VLAN (**vlan** *vlan-id*) that the interface belongs to must be configured.

This function takes effect only for users who go online after this function is successfully configured.

Example

Specify the IP address range 10.1.1.1-10.1.1.10, authentication domain **test**, and VLAN 10 that static users belong to.

```
<HUAWEI> system-view
[HUAWEI] static-user 10.1.1.1 10.1.1.10 domain-name test vlan 10
```

13.6.141 static-user not-update-ip enable

Function

The **static-user not-update-ip enable** command disables the device from updating IP addresses of static users.

The **undo static-user not-update-ip enable** command allows the device to update IP addresses of static users.

By default, the device cannot update IP addresses of static users.

Format

static-user not-update-ip enable

undo static-user not-update-ip enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IP addresses for static users are configured, terminals using these IP addresses are authenticated as static users. After these terminals go online, they may send abnormal ARP packets whose source IP addresses are not the IP addresses of static users to the authentication device. After receiving the packets, the device updates terminal IP addresses in CIB entries. As a result, the terminals are no longer static users and go offline. To prevent this problem, you can run the **static-user not-update-ip enable** command to disable the device from updating IP addresses of static users.

Precautions

When the **undo static-user not-update-ip enable** command is configured and the function of identifying static users through IP addresses is enabled, only the function of identifying static users through IP addresses takes effect.

Example

Disable the device from updating IP addresses of static users.

```
<HUAWEI> system-view
[HUAWEI] static-user not-update-ip enable
```

13.6.142 static-user password

Function

The **static-user password** command sets the password for a static user in authentication.

The **undo static-user password** command restores the default password for the static user.

By default, the password for a static user in authentication not set.

Format

static-user password cipher *password*

undo static-user password

Parameters

Parameter	Description	Value
cipher	Displays a password in cipher text.	-
password	Specifies the password of a static user.	The value is a case-sensitive string without question marks (?) or spaces. The password contains 1 to 128 characters in plain text or 48 to 188 characters in cipher text.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a static user triggers authentication through an ARP packet, you can run the **static-user password** command to set the password for the static user. The access device then sends the password to the authentication server.

Precautions

To improve security, change the default password immediately and update the password periodically. It is recommended that the new password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

This function takes effect only for users who go online after this function is successfully configured.

Example

Configure the password **YsHsjx_202206** for static users.

```
<HUAWEI> system-view
[HUAWEI] static-user password cipher YsHsjx_202206
```


13.6.143 static-user username format-include

Function

The **static-user username format-include** command sets the user name for a static user in authentication.

The **undo static-user username format-include** command restores the default user name for the static user.

By default, the name of a static user consists of **system-name** and **ip-address**. For example, if the access device name is **test** and user IP address is 1.1.1.1, the static user name is **test1.1.1.1**.

Format

static-user username format-include { **ip-address** | **mac-address** | **system-name** }

undo static-user username format-include

Parameters

Parameter	Description	Value
ip-address	Indicates that the user IP address is used as the user name.	-
mac-address	Indicates that the user MAC address is used as the user name.	-
system-name	Indicates that the access device name is used as the user name. To set the device name, run the **sysname** command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a static user triggers authentication through an ARP packet, you can run the **static-user username format-include** command to set the user name for the static user. The access device then sends the user name to the authentication server.

Example

Set the user IP address as the static user name for authentication.

```
<HUAWEI> system-view
[HUAWEI] static-user username format-include ip-address
```

13.6.144 static-user username macaddress format

Function

The **static-user username macaddress format** command sets the user name for authenticating a static user to a MAC address.

The **undo static-user username macaddress format** command restores the default setting.

By default, the user name for authenticating a static user is not set to a MAC address.

Format

static-user username macaddress format { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password-with-macaddress**]

undo static-user username macaddress format

Parameters

Parameter	Description	Value
with-hyphen [**normal**] [**colon**] | **without-hyphen**	Specifies the format of a MAC address. • **with-hyphen**: indicates that the MAC address contains hyphens (-), for example, 0005-e01c-02e3. • **with-hyphen normal**: indicates that the MAC address contains hyphens (-), for example, 00-05-e0-1c-02-e3. • **with-hyphen colon**: indicates that the MAC address contains colons (:), for example, 0005:e01c:02e3. • **with-hyphen normal colon**: indicates that the MAC address contains colons (:), for example, 00:05:e0:1c:02:e3. • **without-hyphen**: indicates that the MAC address does not contain hyphens (-) or colons (:), for example, 0005e01c02e3.	-
uppercase	Configures a MAC address in uppercase format as the user name for authentication. If this parameter is not specified, a MAC address in lowercase format is used.	-

Parameter	Description	Value
password-with-macaddress	Configures a MAC address as the password. If this parameter is not specified, the password configured in the **static-user password cipher** *password* command is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In network deployment, static IP addresses are assigned to dumb terminals such as printers, that is, their users are configured as static users. To authenticate a static user, you can run this command to set the user name and password for authentication to a MAC address. This command takes priority over the **static-user username format-include** { **ip-address** | **mac-address** | **system-name** } command and **static-user password cipher** *password* command.

Example

Set the MAC address with hyphens (-) as the user name and password for authenticating a static user.

```
<HUAWEI> system-view
[HUAWEI] static-user username macaddress format with-hyphen password-with-macaddress
```

13.6.145 url (Portal server template view)

Function

The **url** command configures a URL for a Portal server.

The **undo url** command restores the default configuration.

By default, no URL is configured for a Portal server.

Format

url *url-string*

undo url

Parameters

Parameter	Description	Value
url-string	Specifies a URL for a portal server.	The value is a string of 1 to 247 characters.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the IP address of a Portal server is configured using the **server-ip** command (in the Portal server template view), the Portal server URL (http://*server-ip*) is generated by default on the device. If the actual URL of the Portal server is inconsistent with the default one or the domain name of the Portal server needs to be used for network access, you can run the **url** command to modify the URL of the Portal server on the device.

Precautions

- A Portal server has only one URL.

Example

Set the URL of a Portal server to http://www.***.com in the Portal server template named **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] url http://www.***.com
```

13.6.146 url (URL template view)

Function

The **url** command configures a redirect URL or pushed URL.

The **undo url** command cancels a redirect URL or pushed URL.

By default, no redirect URL or pushed URL is configured.

Format

url [**push-only** | **redirect-only**] *url-string*

undo url [**push-only** | **redirect-only**]

Parameters

Parameter	Description	Value
url-string	Specifies a redirect URL or pushed URL.	The value is a string of 1 to 247 case-sensitive characters without spaces.
push-only	Specifies the URL only as a pushed URL.	-
redirect-only	Specifies the URL only as a redirect URL.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a URL template is created using the **url-template name** command, you can run this command to configure the redirect URL or pushed URL. When a user without network access permission connects to the network, the Portal authentication device redirects the user to the specified URL for authentication. The difference between a redirect URL and a pushed URL is as follows:

- Redirect URL: When a user without network access permission attempts to access the network, the Portal authentication device redirects the user to the redirect URL for authentication.
- Pushed URL: After an authenticated user accesses the network through web for the first time, the access device pushes the web page corresponding to the URL to the user. The web access request from the user is redirected to the specified URL, and then the user is allowed to access network resources.

Precautions

When you configure a URL on the device, question marks (?) are not supported. If a URL contains a question mark (?), you can run the **parameter start-mark #** command in the URL template view to replace the question mark (?) with a number sign (#).

If the **push-only** and **redirect-only** parameters are not specified, the configured URL is used as both a redirect URL and a pushed URL. You can configure pushed URL using the **force-push** command, or use the **url-template** command to bind a URL template to the Portal server template to configure redirect URL.

Example

Set the redirect URL to http://10.1.1.1.


```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.1
```

13.6.147 url-parameter

Function

The **url-parameter** command sets parameters in a URL.

The **undo url-parameter** command deletes parameters in a URL.

By default, a URL does not carry any parameters.

Format

url-parameter { **redirect-url** *redirect-url-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* | **login-url** *url-key url* }*

undo url-parameter

Parameters

Parameter	Description	Value
redirect-url *redirect-url-value*	Specifies the original URL that a user accesses in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces.
user-ipaddress *user-ipaddress-value*	Specifies the user IP address carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces.
sysname *sysname-value*	Specifies the device system name carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces.
user-mac *user-mac-value*	Specifies the user MAC address carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces.

Parameter	Description	Value
login-url *url-key url*	Specifies the login URL of an access device. ● *url-key*: specifies the identification keyword for the login URL sent to the Portal server during redirection. ● *url*: is a specified URL on the access device.	● *url-key*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). ● *url*: The value is a string of 1 to 247 case-sensitive characters without spaces.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

After a URL template is created using the **url-template name** command and URL is configured using the **url** command, you can use the **url-parameter** command to set the parameters in the URL. When a user accesses the Portal server according to the URL, the Portal server obtains user terminal information through the parameters in the URL. The Portal server then provides the corresponding web authentication page for the user according to user terminal information.

In addition, when users are redirected to a website rather than the Portal server according to the pushed URL, the website provides different web pages for the users according to user terminal information carried in the URL.

Example

Set the user MAC address and access device's system name in the URL.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter user-mac usermac sysname test
```


13.6.148 url-parameter mac-address format

Function

The **url-parameter mac-address format** command configures the MAC address format in URL.

The **undo url-parameter mac-address format** command restores the default MAC address format in URL.

By default, the MAC address format in URL is XXXXXXXXXXXX.

Format

url-parameter mac-address format delimiter *delimiter* { **normal** | **compact** }

undo url-parameter mac-address format

Parameters

Parameter	Description	Value
delimiter *delimiter*	Specifies the delimiter in MAC address.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
normal	Sets the MAC address format to XX-XX-XX-XX-XX-XX.	-
compact	Sets the MAC address format to XXXX-XXXX-XXXX.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Portal servers or websites may require different MAC address formats. You can run the **url-parameter mac-address format** command to set MAC address formats in URL to meet the requirements of Portal servers.

Example

Set the delimiter to - and format to XXXX-XXXX-XXXX.


```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter mac-address format delimiter - compact
```

13.6.149 url-template (Portal server template view)

Function

The **url-template** command binds a URL template to a Portal server template.

The **undo url-template** command unbinds a URL template from a Portal server template.

By default, no URL template is bound to a Portal server template.

Format

url-template *url-template* [**ciphered-parameter-name** *ciphered-parameter-name* **iv-parameter-name** *iv-parameter-name* **key cipher** *key-string*]

undo url-template

Parameters

Parameter	Description	Value
url-template	Specifies the name of a URL template.	The value must be an existing URL template name.
ciphered-parameter-name *ciphered-parameter-name*	Specifies the name of the encrypted URL template parameter.	The value is a string of 1 to 16.
iv-parameter-name *iv-parameter-name*	Specifies the encryption vector name of the URL template parameter.	The value is a string of 1 to 16.
key cipher *key-string*	Specifies the shared key for encrypting the URL template parameter.	The value is a string of 1-16 plain-text characters or 48 cipher-text characters.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the parameters of a URL template are configured, the URL template must be bound to a Portal authentication server template so that users can be authenticated on the Portal authentication server corresponding to the redirect URL.

To ensure security, you can encrypt the parameter information in the URL template bound to the Portal server template.

Prerequisites

A URL template has been created using the **url-template name** command.

Precautions

If a URL template is bound to the Portal authentication server template and the **url** command is executed to configure the redirect URL corresponding to the Portal authentication server, only the parameters in the URL template take effect.

The device support encryption of parameter information in the URL template only when it connects to the Huawei Agile Controller-Campus or iMaster NCE-Campus.

Example

Bind the URL template **abc** to the Portal authentication server template.

```
<HUAWEI> system-view
[HUAWEI] url-template name abc
[HUAWEI-url-template-abc] quit
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] url-template abc
```

13.6.150 url-template name

Function

The **url-template name** command creates a new URL template or enter an existing URL template view.

The **undo url-template name** command deletes a URL template.

By default, no URL template exists on the device.

Format

url-template name *template-name*

undo url-template name *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of a URL template.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a Portal authentication server template is created using the **web-auth-server** command, you can bind a URL template to the Portal authentication server template. The URL template contains the redirect URL and redirect URL parameters.

The **url-template name** command creates a new URL template or enter an existing URL template view.

Example

Create a URL template named **test** and enter the template view.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
```

13.6.151 user-group

Function

The **user-group** command creates a user group or displays the user group view.

The **undo user-group** command deletes a user group.

By default, no user group is configured.

Format

user-group *group-name*

undo user-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a user group.	The value is a string of 1-64 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practical NAC applications, there are many access users and a large number of ACL rules need to be configured for each user. However, the number of user types is limited.

You can run the **user-group** command to create user groups on the device and associate each user group to a group of ACL rules (for details, see **acl-id**). In this way, users in the same group share a group of ACL rules. The limited ACL resources can support a large number of access users.

NOTE

When the user group function is enabled on models except the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, ACL rules are delivered to each user and the user group function cannot be used to save ACL resources.

Precautions

- When you create a user group, ensure that the user group name is different from the number of an existing ACL. You can run the **display acl all** command to view the configuration of all ACL rules on the device.
- If you want to delete the user group when the ACL bound to the user takes effect, run the **cut access-user user-group** *group-name* command to disconnect all users bound to the user group, and run the **undo user-group** *group-name* **enable** command to disable the user group function.
- The priority of the user group authorization information delivered by the authentication server is higher than that of the user group authorization information applied in the AAA domain. If the user group authorization information delivered by the authentication server cannot take effect, the user group authorization information applied in the AAA domain is used. For example, if only user group B is configured on the device and the group authorization information is applied in the AAA domain when the authentication server delivers authorization information about user group A,

the authorization information about user group A cannot take effect and the authorization information about user group B is used. To make the user group authorization information delivered by the authentication server take effect, ensure that this user group is configured on the device.

Example

Create a user group **test1**.

```
<HUAWEI> system-view
[HUAWEI] user-group test1
```

13.6.152 user-group enable

Function

The **user-group enable** command enables the user group function.

The **undo user-group enable** command disables the user group function.

By default, the user group function is disabled.

Format

user-group *group-name* **enable**

undo user-group *group-name* **enable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a user group.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user group has been created using the **user-group** command, run the **user-group enable** command to enable the user group function.

Precautions

After the user group function is enabled, the binding relationship between a user group and an ACL cannot be modified.

If the user group function is not enabled, users going online through Layer 2 interfaces can access the network without restriction, while users going online through VLANIF interfaces are not allowed to access the network.

Example

Enable the user group **test**.

```
<HUAWEI> system-view
[HUAWEI] user-group test enable
```

13.6.153 user-sync

Function

The **user-sync** command enables user information synchronization.

The **undo user-sync** command disables user information synchronization.

By default, user information synchronization is disabled.

Format

user-sync [**interval** *interval-period* | **max-times** *times*] *

undo user-sync

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the user information synchronization interval.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 300.
max-times *times*	Specifies the maximum number of user information synchronization failures.	The value is an integer that ranges from 2 to 255. The default value is 3.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If communication is interrupted because the network between the device and Portal server is disconnected or the Portal server is faulty, online Portal

authentication users cannot go offline. Therefore, user information on the device and on the Portal server may be inconsistent and accounting may be inaccurate.

The **user-sync** command enables user information synchronization so that user information on the device and Portal server is synchronized at intervals to ensure user information consistency.

NOTE

During information synchronization, the device does not disconnect the user immediately after detecting that the device has certain user information while the server does not have such information. Instead, the device disconnects the user when the maximum number of user information synchronization failures is reached.

Precautions

If users go online during the keepalive interval of the Portal server, the Portal server does not have their entries. After the Portal server goes Up and starts synchronizing user information, the device does not disconnect these users even if synchronization fails. The device retails these users until next time these users go online and performs Portal authentication, ensuring good user experience.

The value of *interval-period***times* configured on the device must be greater than the interval for the Portal server to send synchronization packets. Otherwise, the device forces users offline when it cannot receive any synchronization packet from the Portal server after the maximum failure number is reached.

Example

Enable user information synchronization in the Portal server template **abc**, set the interval for user information synchronization to 100s, and set the maximum number of synchronization failures to 5.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] user-sync interval 100 max-times 5
```

13.6.154 user-vlan (user group view)

Function

The **user-vlan** command configures a user group VLAN.

The **undo user-vlan** restores the default setting.

By default, no user group VLAN is configured.

Format

user-vlan *vlan-id*

undo user-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a user group VLAN.	The value is an integer that ranges from 1 to 4094.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a user group is created using the **user-group** command, you can run the **user-vlan** command to configure a user group VLAN, so that users in different user groups have different network access permissions. When a user in a user group goes online, the user is added to the user group VLAN to obtain the network access permission of this user group.

Prerequisites

The user group VLAN has been created using the **vlan** command.

Precautions

- An authorized VLAN cannot be delivered to online Portal users.
- The **user-vlan** command does not take effect for the users who are already online.
- Access switches will send untagged frames to users in the user VLAN even when interfaces connected users are added to this user VLAN in tagged mode.

Example

Set the VLAN of the user group **abc** to 10.

```
<HUAWEI> system-view
[HUAWEI] user-group abc
[HUAWEI-user-group-abc] user-vlan 10
```

13.6.155 vpn-instance (Portal server template view)

Function

The **vpn-instance** command configures a VPN instance used for communication between the device and Portal server.

The **undo vpn-instance** command restores the default setting.

By default, no VPN instance is configured for communication between the device and Portal server.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VPN implements interconnection within the same department and between different departments in an enterprise. To enable the Portal authentication service in the VPN, run the **vpn-instance** command to bind a Portal server template to a VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

The VPN instance bound to the Portal server template must be the same as that bound to the Portal server; otherwise, the device cannot perform Portal authentication for access users.

The users in VPN instances bound to different Portal server templates cannot use the same IP addresses because users with the same IP addresses cannot go online or offline.

Example

Bind the Portal server template **abc** to the VPN instance **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] vpn-instance test
```


13.6.156 web-auth-server version

Function

The **web-auth-server version** command sets the Portal protocol version supported by the device.

The **undo web-auth-server version** command restores the default setting.

By default, the device supports both the versions V1.0 and V2.0.

Format

web-auth-server version v2 [**v1**]

undo web-auth-server version

Parameters

Parameter	Description	Value
v2	Indicates that the device supports the Portal protocol version V2.0. The major version currently used is V2.0.	-
v1	Indicates that the device supports the Portal protocol version V1.0.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Currently, the Portal protocol has two versions: V1.0 and V2.0. The device and Portal server must use the Portal protocol of the same version to ensure normal communication. You can run the **web-auth-server version** command to set the Portal protocol version supported by the device.

NOTE

The version V2.0 is widely used currently.

To ensure smooth communication, the device supports both versions by default.

Example

Configure the device to use only the Portal protocol V2.0.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server version v2
```


13.6.157 web-auth-server (interface view)

Function

The **web-auth-server** command binds a Portal server template to an interface.

The **undo web-auth-server** command unbinds a Portal server template from an interface.

By default, no Portal server template is bound to an interface.

Format

- VLANIF interface view:

  web-auth-server *server-name* [*bak-server-name*] { **direct** | **layer3** }

  undo web-auth-server [*server-name* [*bak-server-name*]] { **direct** | **layer3** }
- Layer 3 Ethernet interface view: (Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this)

  web-auth-server *server-name* [*bak-server-name*] **layer3**

  undo web-auth-server [*server-name* [*bak-server-name*] **layer3**]

Parameters

Parameter	Description	Value
server-name	Specifies the name of the Portal server template.	The value must be an existing Portal server template name.
bak-server-name	Specifies the name of the secondary Portal server template. **NOTE** The name of the secondary Portal server template cannot be configured to the command-line keywords **direct** and **layer3**.	The value must be an existing Portal server template name.
direct	Indicates Layer 2 authentication.	-
layer3	Indicates Layer 3 authentication.	-

Views

VLANIF interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A configured Portal server template must be bound to the interface. In this way, the users connected to this interface can be authenticated by the Portal server.

When the Portal server template is bound to the interface using the **web-auth-server** command and a user attempts to access charged network resources, the user is forcibly redirected to the configured Portal authentication page for Portal authentication.

After the primary and secondary Portal server templates are configured, the users who send HTTP requests are redirected to the network access page provided by the secondary Portal server when the primary Portal server is faulty or cannot be accessed. This meets the users' network access requirements. This function can take effect only when the primary Portal server detection function is enabled using the **server-detect** command and heartbeat detection is enabled on the Portal server.

Portal authentication modes are as follows:

- **direct**: When there is no Layer 3 forwarding device between the user and device, the device can learn the user's MAC address. The device identifies the user using the MAC address.
- **layer3**: Whether Layer 3 forwarding devices exist between the user and device, the MAC address table of the device cannot learn the user's MAC address. The device identifies the user using the IP address uniquely.

Prerequisites

A Portal server template has been created using the **web-auth-server** command and an IP address has been configured for the Portal server using the **server-ip** command.

Precautions

- You can bind only one Portal server template to an interface. To modify a Portal server template that has been bound to an interface, remove the template from the interface, modify the template, and bind the modified template to the interface again.
- If 802.1X authentication, MAC address authentication, MAC address bypass authentication is enabled on a Layer 2 interface, this command cannot be executed on the VLANIF interface of a VLAN to which the Layer 2 interface is added.
- This command does not take effect on the VLANIF interface corresponding to the super VLAN.

Example

Bind the Portal server template Server1 to VLANIF10, and set the authentication mode to Layer 2 authentication.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] web-auth-server Server1
[HUAWEI-web-auth-server-Server1] server-ip 10.10.1.1
```



```
[HUAWEI-web-auth-server-Server1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] web-auth-server Server1 direct
```

13.6.158 web-auth-server listening-port

Function

The **web-auth-server listening-port** command sets the number of the port through which a device listens on Portal protocol packets.

The **undo web-auth-server listening-port** command restores the default listening port.

By default, the device uses port 2000 to listen on Portal protocol packets.

Format

web-auth-server listening-port *port-number*

undo web-auth-server listening-port

Parameters

Parameter	Description	Value
port-number	Specifies the number of the listening port.	The value is an integer that ranges from 1024 to 55535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device exchanges user authentication information with the Portal server using the Portal protocol, you must configure the listening port on the device to receive Portal packets.

You can run the **web-auth-server listening-port** command to set the number of the port through which the device listens on Portal packets. The port number must be the same as the destination port number in Portal packets sent by the Portal server and must be unique.

NOTE

If a specified port is occupied by another service or is a reserved port, the configuration fails. Ensure that the specified port is available when running this command.

Example

Set the number of the port through which a device listens on Portal protocol packets to 3000.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server listening-port 3000
```

13.6.159 web-auth-server reply-message

Function

The **web-auth-server reply-message** command enables the device to transparently transmit users' authentication responses sent by the authentication server to the Portal server.

The **undo web-auth-server reply-message** command disables the device from transparently transmitting users' authentication responses sent by the authentication server to the Portal server.

By default, the device transparently transmits users' authentication responses sent by the authentication server to the Portal server.

Format

web-auth-server reply-message

undo web-auth-server reply-message

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The AAA server requires that the authentication messages sent to the Portal server contain the authentication reply; therefore, the **web-auth-server reply-message** command is required. In certain situations, the authentication messages are not required to carry the reply. In this case, run the **undo web-auth-server reply-message** command.

By default, the device directly forwards the authentication result message from the RADIUS server to the Portal server without processing. This is called transparent transmission.

Example

Disable the device from transparently transmitting users' authentication responses to the Portal server.

```
<HUAWEI> system-view
[HUAWEI] undo web-auth-server reply-message
```

13.6.160 web-auth-server (system view)

Function

The **web-auth-server** command creates a Portal server template or displays the Portal server template view.

The **undo web-auth-server** command deletes a Portal server template.

By default, no Portal server template is created.

Format

web-auth-server *server-name*

undo web-auth-server *server-name*

Parameters

Parameter	Description	Value
server-name	Specifies the name of a Portal server.	The value is a string of 1 to 31 case-sensitive characters without spaces. **NOTE** *server-name* cannot be set to listening-port, reply-message, version, or the first character or several leftmost characters of these character strings.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an unauthenticated Portal user goes online, the device forces the user to log in to a specified website (also called the Portal website). The user can access

resources in the Portal website for free. When the user attempts to access charged network resources, the user must pass authentication on the Portal website. The specific process is as follows:

1. The unauthorized user opens Internet Explorer and enters a URL in the address box. When receiving the HTTP request sent by the user, the device redirects it to the Portal authentication page of the Portal server.
2. The user enters user information on the authentication page or in the authentication dialog box, and the Portal server forwards the user information to the device.
3. After receiving the user information from the Portal server, the device sends the information to the authentication server for authentication and accounting.
4. After the user is authenticated, the device allows the user to access the Internet if no security policy is enforced.

After a Portal server template is created on the device by using the **web-auth-server** command, run other commands to create a route from the device to the Portal server.

Follow-up Procedure

Run the following commands to configure related attributes of the Portal server template:

- Run the **server-ip** command to configure an IP address for the Portal server.
- Run the **url** command to configure a URL of the Portal server.
- Run the **port** command to set the port number that a Portal server uses to receive notification packets from the device.
- Run the **shared-key** command configures the shared key that the device uses to exchange information with the Portal server.

Precautions

You are advised to back up the Portal server data to prevent authentication failure caused by the Portal server fault.

If you want to run the **undo web-auth-server** command to delete a Portal server template, ensure that the Portal server template is not bound to the interface.

Example

Create the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
```

13.6.161 web-redirection disable (Portal server template view)

Function

The **web-redirection disable** command disables the Portal authentication redirection function.

The **undo web-redirection disable** command enables the Portal authentication redirection function.

By default, the Portal authentication redirection function is enabled.

Format

web-redirection disable

undo web-redirection disable

Parameters

None

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

The device redirects all unauthenticated users to the Portal authentication page when the users send access requests to external networks. For example, when the user needs to enter the URL of the authentication page manually, the **web-redirection disable** command can be executed so that unauthorized users are not forcibly redirected to the Portal authentication page.

NOTE

If the Portal server template has been bound to the VLANIF interface, this command cannot be executed.

After this command is executed, if multiple server IP addresses are configured in the Portal server template and no URL is configured, the device does not display error information when the Portal server template is bound to the VLANIF interface.

Example

Disable the Portal authentication redirection function.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server nac
[HUAWEI-web-auth-server-nac] web-redirection disable
```

13.7 Policy Association Configuration Commands

13.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.7.2 access-user arp-detect control-point mac-ip enable

Function

The **access-user arp-detect control-point mac-ip enable** command configures the source IP address and source MAC address of detection packets sent by an AS to be the same as those used by an authentication control device for detection.

The **undo access-user arp-detect control-point mac-ip enable** command cancels the configuration.

By default, the source IP address and source MAC address of detection packets sent by an AS are not configured to be the same as those used by an authentication control device for detection.

Format

access-user arp-detect control-point mac-ip enable

undo access-user arp-detect control-point mac-ip enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In policy association and SVF scenarios, you can run this command on an authentication control device to configure the source IP address and source MAC address of detection packets sent by an AS to be the same as those used by the authentication control device for detection, simplifying the configuration on the AS.

Precautions

This command is supported only on authentication control devices.

This function takes effect only for users who go online after this command is successfully configured.

For details about how to configure source addresses of detection packets sent by an authentication control device, see "Setting the Source Address of Offline Detection Packets" in the "NAC Configuration" chapter.

Example

Configure the source IP address and source MAC address of detection packets sent by an AS to be the same as those used by an authentication control device for detection.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect control-point mac-ip enable
```

13.7.3 as access controller ip-address

Function

The **as access controller ip-address** command specifies an IP address for an authentication control device on an authentication access device.

The **undo as access controller ip-address** command deletes the IP address specified for an authentication control device from an authentication access device.

By default, no IP address is specified for an authentication control device on an authentication access device.

Format

as access controller ip-address *ip-address*

undo as access controller ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for an authentication control device.	The value is in dotted decimal notation.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the policy association solution is deployed, authentication access devices and authentication control devices establish connections through CAPWAP tunnels. When an authentication access device dynamically obtains an IP address through the DHCP server, Option 43 is used to notify the authentication access device of the IP address for the authentication control device with which the

authentication access device establishes a CAPWAP tunnel. When an IP address is statically configured for an authentication access device, the **as access controller ip-address** *ip-address* command is used to specify the IP address for the authentication control device with which the authentication access device establishes a CAPWAP tunnel.

Precautions

This command is supported only on authentication access devices.

Example

Specify an IP address for an authentication control device.

```
<HUAWEI> system-view
[HUAWEI] as access controller ip-address 10.1.1.1
```

13.7.4 as access interface

Function

The **as access interface** command specifies source interface for establishing CAPWAP tunnels on an authentication access device.

The **undo as access interface** command deletes the source interface specified for establishing CAPWAP tunnels from an authentication access device.

By default, no source interface is specified for establishing CAPWAP tunnels on an authentication access device.

Format

as access interface vlanif *vlan-id*

undo as access interface

Parameters

Parameter	Description	Value
vlanif *vlan-id*	Specifies a source interface for establishing CAPWAP tunnels.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the policy association solution is deployed, CAPWAP tunnels are used for connection establishment, user association, message communication, user authorization policy delivery, and user synchronization between authentication control devices and authentication access devices. On an authentication access device, run the **as access interface vlanif** *vlan-id* command to specify a source interface for establishing CAPWAP tunnels.

Precautions

This command is supported only on authentication access devices.

The management VLAN of the CAPWAP tunnel cannot be the same as the management VLAN or PnP VLAN of the switches managed by iMaster NCE-Campus.

In policy association, the management VLAN of a CAPWAP tunnel connects authentication access devices to the network. It is not recommended to perform other service configurations except basic configurations in the management VLAN and the corresponding VLANIF interface. If such configurations are performed, authentication access devices may fail to connect to the network.

Example

Specify a source interface for establishing CAPWAP tunnels.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] quit
[HUAWEI] as access interface vlanif 10
```

13.7.5 authentication access-point

Function

The **authentication access-point** command enables remote authentication access control on the interface of an authentication access device.

The **undo authentication access-point** command disables remote authentication access control on the interface of an authentication access device.

By default, remote access control is disabled on the interface of an authentication access device.

Format

authentication access-point [**open**]

undo authentication access-point [**open**]

Parameters

Parameter	Description	Value
open	Disables right control of the access point.	-

Views

Ethernet interface view, MultiGE interface view, 40GE interface view, GE interface view, XGE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you deploy policy association, configure the interface of each authentication access device as the access point and enable remote access control on the interface.

To configure right control on an authentication control device instead of an authentication access device, you can disable right control of the access point on the authentication access device (by specifying the **open** parameter).

Precautions

This command is supported only on authentication access devices.

NOTE

The **authentication access-point open** and **authentication access-point** command must be run together; otherwise, the **authentication access-point open** command cannot take effect.

The interface types vary according to device models.

If there is a terminal with one MAC address and multiple IP addresses on the live network, you need to configure the function of identifying static users through IP addresses on the authentication control device. However, because the authentication access device cannot generate multiple entries for the terminal, you cannot implement right control on the authentication access device. In this case, you need to disable right control of the access point on the authentication access device. Otherwise, packets of the terminal will not be forwarded.

Example

Configure GE0/0/1 as the access point.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication access-point
```

13.7.6 authentication access-point max-user

Function

The **authentication access-point max-user** command sets the maximum number of access users allowed on an interface of an authentication access device.

The **undo authentication access-point max-user** command restores the default setting.

By default, an authentication access device does not limit the maximum number of users who are allowed to log in through its interfaces.

Format

authentication access-point max-user *max-user-number*

undo authentication access-point max-user

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of access users allowed on an interface of an authentication access device.	The value is an integer that ranges from 1 to 512 for S6735-S, S6720-EI, and S6720S-EIfrom 1 to 1000 for S5731-S and S5731S-S, from 1 to 1024 for S5731-H, S6730-H, S6730S-H, S5731S-H, S5732-H, S6730-S, and S6730S-S, and from 1 to 300 for other models.

Views

Ethernet interface view, MultiGE interface view, 40GE interface view, GE interface view, XGE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To limit the maximum number of access users allowed on an interface of an authentication access device, run the **authentication access-point max-user** command.

Precautions

This command is supported only on authentication access devices.

This command takes effect only for users who attempt to log in for the first time.

The interface types vary according to device models.

Example

Set the maximum number of access users allowed on GE 0/0/1 to 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication access-point max-user 100
```


13.7.7 authentication associate alarm-restrain enable

Function

The **authentication associate alarm-restrain enable** command enables an authentication access device to suppress alarms that are generated due to excess associated users.

The **undo authentication associate alarm-restrain enable** command disables alarm suppression.

By default, an authentication access device is enabled to suppress alarms that are generated due to excess associated users.

Format

authentication associate alarm-restrain enable

undo authentication associate alarm-restrain enable

Parameters

None

Views

System view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If associated users fail to log in to an authentication access device due to the configured limitation on the access number, the device generates alarms about the login failure event.

These alarms consume device resources and affect system performance. To prevent the device from generating too many repeated alarms in a short period, run the **authentication associate alarm-restrain enable** command to enable suppression on these alarms. The device then does not generate alarms of the same type within a specified suppression period (set using the **authentication associate alarm-restrain period** command).

Precautions

This command is supported only on authentication access devices.

Example

Enable an authentication access device to suppress alarms that are generated due to excess associated users.


```
<HUAWEI> system-view
[HUAWEI] authentication associate alarm-restrain enable
```

13.7.8 authentication associate alarm-restrain period

Function

The **authentication associate alarm-restrain period** command sets a suppression period for alarms that an authentication access device generates due to excess associated users.

The **undo authentication associate alarm-restrain period** command restores the default setting.

By default, an authentication access device suppresses such alarms for 300 seconds.

Format

authentication associate alarm-restrain period *period-value*

undo authentication associate alarm-restrain period

Parameters

Parameter	Description	Value
period-value	Specifies a suppression period for alarms that an authentication access device generates due to excess associated users.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an authentication access device is enabled to suppress alarms that are generated due to excess associated users using the **authentication associate alarm-restrain enable** command, run the **authentication associate alarm-restrain period** command to set a suppression period for these alarms. The device then does not generate alarms of the same type within the suppression period.

Precautions

This command is supported only on authentication access devices.

Example

Set the suppression period to 600s for alarms that an authentication access device generates due to excess associated users.

```
<HUAWEI> system-view
[HUAWEI] authentication associate alarm-restrain period 600
```

13.7.9 authentication control-point

Function

The **authentication control-point** command configures an interface as the control point.

The **undo authentication control-point** command restores the default setting.

By default, an interface does not function as a control point.

Format

authentication control-point [**open**]

undo authentication control-point

Parameters

Parameter	Description	Value
open	Enables the forwarding function of the control point.	-

Views

VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When policy association is configured, the interface on an authentication control device is configured as the control point. If the **open** parameter is configured, the control point directly forwards user traffic. If the **open** parameter is not configured, the control point manages the forwarding rights for user traffic through NAC authentication.

Precautions

- This command is supported only on authentication control devices.
- When the VLANIF interface is configured as the NAC authentication interface, the VLANIF interface and its mapping physical interface must be configured as control points. However, NAC authentication cannot be configured on the physical interface. The **open** parameter cannot be configured for a VLANIF interface.
- When the interface below functions as the control point, it can only directly forward user traffic. That is, only the **authentication control-point open** command can be configured.
  - An interface on the S6720S-SS6720-EI or S6720S-EI, S6735-S
  - An Eth-Trunk interface containing interfaces on the S6720S-SS6720-EI or S6720S-EI, S6735-S

Example

Configure GE0/0/1 as the control point.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication control-point
```

13.7.10 authentication open ucl-policy enable

Function

The **authentication open ucl-policy enable** command configures a control point where the **authentication control-point open** command has been configured to filter user traffic based on a user ACL before forwarding the traffic.

The **undo authentication open ucl-policy enable** command restores a control point where **authentication control-point open** has been configured to directly forwarding user traffic.

By default, a control point where **authentication control-point open** has been configured directly forwards user traffic.

NOTE

Only the S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S5731-H, S5731S-HX series cards support this command.

Format

authentication open ucl-policy enable

undo authentication open ucl-policy enable

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is applicable to the following scenarios:

- When only independent policy association is used, the **authentication control-point open** command has been configured on a control point.
- When policy association is used in an SVF system, the **authentication control-point open** command is configured on a control point by default.

A control point directly forwards traffic from wired users who go online on an interface of the access device without authentication and the traffic from users who pass NAC authentication but do not obtain the authority granted to the UCL group and the traffic from wireless users in direct forwarding mode. To enable the control point to filter user traffic based on a user ACL, run the **authentication open ucl-policy enable** command.

Precautions

This command can be executed only on the control device.

- In versions earlier than V200R012, rRun the **traffic-filter inbound acl** { *acl-number* | **name** *acl-name* } command on the control device to configure user ACL-based packet filtering before running the **authentication open ucl-policy enable** command.
- In V200R012 and later versions, the **authentication open ucl-policy enable** command is optional if the **traffic-filter inbound acl** { *acl-number* | **name** *acl-name* } command has been configured on the control device to configure user ACL-based packet filtering.

  To disable user ACL-based packet filtering, run the **undo traffic-filter inbound acl** { *acl-number* | **name** *acl-name* } and **undo authentication open ucl-policy enable** commands.

Example

Configure the control point GE1/0/1 where the **authentication control-point open** command has been configured to filter user traffic based on a user ACL before forwarding the traffic.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] authentication control-point open
[HUAWEI-GigabitEthernet1/0/1] authentication open ucl-policy enable
```

13.7.11 authentication speed-limit

Function

The **authentication speed-limit** command configures the rate limit for an authentication access device to send user association and disassociation request messages.

The **undo authentication speed-limit** command restores the default rate limit for an authentication access device to send user association and disassociation request messages.

By default, an authentication access device sends a maximum of 60 user association and disassociation request messages within 30 seconds.

Format

authentication speed-limit max-num *max-num-value* **interval** *interval-value*

undo authentication speed-limit

Parameters

Parameter	Description	Value
max-num *max-num-value*	Specifies the maximum number of user association and disassociation request messages.	The value is an integer that ranges from 1 to 65535. The default value is 60.
interval *interval-value*	Specifies the interval for an authentication access device to send user association and disassociation request messages.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 30.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An authentication control device can connect to multiple authentication access devices. If the rate limit for an authentication access device to send user association and disassociation request messages is not specified, there will be a heavy load on the authentication control device. You can run this command to adjust the rate limit.

Precautions

This command is supported only on authentication access devices.

In an SVF system, commands cannot be configured on authentication access devices. When the access rate of users is high, they may fail to go online due to a

rate limit. To lower the rate limit, run the **direct-command** command on the authentication control device to deliver the **authentication speed-limit** command configuration to the authentication access devices. This requires that the authentication access devices run V200R013C00 or a later version.

Example

Configure the authentication access device to send a maximum of 100 association and disassociation request messages within 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication speed-limit max-num 100 interval 10
```

13.7.12 control-down offline delay (authentication access device)

Function

The **control-down offline delay** command configures the user logout delay on an authentication access device when a control tunnel is faulty.

The **undo control-down offline delay** command deletes the user logout delay on an authentication access device when a control tunnel is faulty.

By default, the user logout delay is not configured on an authentication access device when a control tunnel is faulty, indicating that the users on an authentication access device go offline immediately when a control tunnel is faulty.

Format

control-down offline delay { *delay-value* | **unlimited** }

undo control-down offline delay

Parameters

Parameter	Description	Value
delay-value	Specifies the user logout delay when a control tunnel is faulty.	The value is an integer that ranges from 1 to 60, in seconds.
unlimited	Specifies the user logout delay as unlimited. That is, users do not go offline when a control tunnel is faulty.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **control-down offline delay** command to configure the user logout delay on an authentication access device when a control tunnel is faulty. In this way, the users will not directly go offline upon a tunnel fault. If the fault persists after the delay, the users go offline; if the fault is rectified within the delay, the users keep online.

Precautions

This command is supported only on authentication access devices.

You are advised to configure the same user logout delay on authentication control devices and authentication access devices.

Example

Configure the user logout delay to 10 seconds on an authentication access device after the control tunnel is faulty.

```
<HUAWEI> system-view
[HUAWEI] control-down offline delay 10
```

13.7.13 control-down offline delay (authentication control device)

Function

The **control-down offline delay** command configures the user logout delay on an authentication control device when a control tunnel is faulty.

The **undo control-down offline delay** command deletes the user logout delay on an authentication control device when a control tunnel is faulty.

By default, the user logout delay is not configured on an authentication control device when a control tunnel is faulty, indicating that users on an authentication control device go offline immediately when a control tunnel is faulty.

Format

control-down offline delay { *delay-value* | **unlimited** }

undo control-down offline delay

Parameters

Parameter	Description	Value
delay-value	Specifies the user logout delay when a control tunnel is faulty.	The value is an integer that ranges from 1 to 60, in seconds.
unlimited	Specifies the user logout delay as unlimited. That is, users do not go offline when a control tunnel is faulty.	-

Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **control-down offline delay** command to configure the user logout delay on an authentication control device when a control tunnel is faulty. In this way, the users will not directly go offline upon a tunnel fault. If the fault persists after the delay, the users go offline; if the fault is rectified within the delay, the users keep online.

Precautions

This command is supported only on authentication control devices.

You are advised to configure the same user logout delay on authentication control devices and authentication access devices.

When you configure users not to go offline upon a channel tunnel failure, you also need to configure **link-down offline delay unlimited** command in the authentication profile view.

Example

Configure the user logout delay to 10 seconds on GE0/0/1 of the authentication control device after a control tunnel is faulty.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] control-down offline delay 10
```


13.7.14 display access-user as-name

Function

The **display access-user as-name** command displays information about online users on a specified authentication access device.

Format

display access-user as-name *as-name*

Parameters

Parameter	Description	Value
as-name	Specifies the name of an authentication access device.	The value is the name of an existing authentication access device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about online access users on an authentication control device.

The actual name of an authentication access device may differ from the name displayed on the authentication control device (using the **display as all** command). When an authentication access device goes online, its name is processed as follows:

- If the authentication access device uses the default name, its name is changed to *default name-MAC address of the authentication access device* on the authentication control device.
- If the authentication access device name contains spaces or double quotation masks ("), the spaces are changed to hyphens (-) and the double quotation masks (") are changed to single quotation masks (') on the authentication control device.

Example

Display information about users on the authentication access device **test_as**.

```
<HUAWEI> display access-user as-name test_as
--------------------------------------------------------------------------------
```



```
UserID Username               IP address      MAC            Status
--------------------------------------------------------------------------------
16019  fdsa@none              192.168.6.5     xxxx-xxxx-xxxx Success
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

NOTE

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

Table 13-120 Description of the **display access-user as-name** command output

Item	Description
UserID	ID that is assigned to a user after the user goes online.
Username	Name of a user.
IP address	IP address of a user.
MAC	MAC address of a user.
Status	Status of a user.

13.7.15 display access-user arp-detect control-point mac-ip

Function

The **display access-user arp-detect control-point mac-ip** command displays whether the source IP address and source MAC address of detection packets sent by an AS are configured to be the same as those used by an authentication control device for detection.

Format

display access-user arp-detect control-point mac-ip

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check whether the source IP address and source MAC address of detection packets sent by an AS are configured to be the same as those used by an authentication control device for detection.

Precautions

This command is supported only on authentication control devices.

Example

Display whether the source IP address and source MAC address of detection packets sent by an AS are configured to be the same as those used by an authentication control device for detection.

```
<HUAWEI> display access-user arp-detect control-point mac-ip
 access-user arp-detect control-point mac-ip: Enable
```

Table 13-121 Description of the **display access-user arp-detect control-point mac-ip** command output

Item	Description
access-user arp-detect control-point mac-ip	Whether the source IP address and source MAC address of detection packets sent by an AS are configured to be the same as those used by an authentication control device for detection: • Enable: yes • Disable: no

13.7.16 display associate-user

Function

The **display associate-user** command displays associated users on devices.

Format

display associate-user

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check associated users on authentication access devices and authentication control devices.

Precautions

There are no longer associated users on authentication control devices after the users are successfully authenticated or added to domains. You can run the **display access-user** command to check user information.

Example

Display the associated users on an authentication control device.

```
<HUAWEI> display associate-user
------------------------------------------------------------------------
UserID IP address       MAC            SA MAC
------------------------------------------------------------------------
27     192.168.12.1     00e0-fc88-143f 00e0-fc43-e00a
------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 13-122 Description of the **display associate-user** command output

Item	Description
UserID	ID that is assigned to a user after the user is associated.
IP address	IP address of a user.
MAC	MAC address of a user.
SA MAC	MAC address of an authentication access device.

Display the associated users on an authentication access device.

```
<HUAWEI> display associate-user
------------------------------------------------------------------------------
UserID IP address       MAC            Status       Trigger type
------------------------------------------------------------------------------
27     192.168.12.1     00e0-fc88-143f Associated    Arp
------------------------------------------------------------------------------
Total: 1, printed: 1
```


Table 13-123 Description of the **display associate-user** command output

Item	Description
UserID	ID that is assigned to a user after the user is associated.
IP address	IP address of a user.
MAC	MAC address of a user.
Status	Status of a user. • Up: indicates that the authentication access device has received the authentication success notification from the authentication control device and enabled data forwarding rights for users. • Associated: indicates that the authentication access device has received the association success response from the authentication control device and is waiting for the authentication success notification from the authentication control device. • Idle: indicates that the authentication access device detects that the user has been connected and periodically sends an association request or is waiting for the association response from the authentication control device. • Deleting: indicates that the user has been added to the logout queue and is waiting for logout.

Item	Description
Trigger type	Triggering type. • Arp: indicates that ARP packets are sent to trigger creation of the association table. • Dot1x: indicates that dot1x packets are sent to trigger creation of the association table. • Http: indicates that HTTP packets are sent to trigger creation of the association table. • Dhcp: indicates that DHCP packets are sent to trigger creation of the association table. • Dhcpv6: indicates that DHCPv6 packets are sent to trigger creation of the association table. • Nd: indicates that Nd packets are sent to trigger creation of the association table.

13.7.17 display associate-user statistics

Function

The **display associate-user statistics** command displays statistics about associated users on an interface.

Format

display associate-user statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about associated users on a specified interface. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check statistics about associated users on an interface, run the **display associate-user statistics** command.

Precautions

This command is supported only on authentication access devices.

Example

Display statistics about associated users on an interface.

```
<HUAWEI> display associate-user statistics
--------------------------------------------------------------------------------
Interface                    number
--------------------------------------------------------------------------------
GigabitEthernet0/0/1         3
TotalNumber                  3
--------------------------------------------------------------------------------
  Total 1
```

Table 13-124 Description of the **display associate-user statistics** command output

Item	Description
Interface	Interface that functions as an access point.
number	Number of associated users on a specified access point.
TotalNumber	Total number of associated users on all access points.
Total: *m*	Total number of interfaces with which users are associated.

13.7.18 display authentication associate

Function

The **display authentication associate** command displays the global configurations of associated users.

Format

display authentication associate

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the global configurations of associated users, run the **display authentication associate** command. The command output contains the suppression status of alarms that an authentication access device generates due to excess associated users and the configured alarm suppression period.

Precautions

This command is supported only on authentication access devices.

Example

Display the global configurations of associated users.

```
<HUAWEI> display authentication associate
 authentication associate alarm-restrain: Enable
 authentication associate alarm-restrain period: 300
```

Table 13-125 Description of the **display authentication associate** command output

Item	Description
authentication associate alarm-restrain	Suppression status of alarms that an authentication access device generates due to excess associated users: • Enable • Disable To configure a suppression status, run the **authentication associate alarm-restrain enable** command.

Item	Description
authentication associate alarm-restrain period	Suppression period for alarms that an authentication access device generates due to excess associated users. To configure a suppression period, run the **authentication associate alarm-restrain period** command.

13.7.19 display authentication associate alarm-restrain-table

Function

The **display authentication associate alarm-restrain-table** command displays suppression table information of alarms that are generated due to excess associated users.

Format

display authentication associate alarm-restrain-table { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays alarm suppression table information on all interfaces.	-
interface *interface-type interface-number*	Displays alarm suppression table information on a specified interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an authentication access device is enabled to suppress alarms that are generated due to excess associated users using the **authentication associate alarm-restrain enable** command, run the **display authentication associate alarm-restrain-table** command to check the alarm suppression table information.

Precautions

This command is supported only on authentication access devices.

Example

Display alarm suppression table information on all interfaces.

```
<HUAWEI> display authentication associate alarm-restrain-table all
--------------------------------------------------------------------------------
Interface                   alarm time
--------------------------------------------------------------------------------
GigabitEthernet0/0/1        --
--------------------------------------------------------------------------------
  Total 1
```

Table 13-126 Description of the **display authentication associate alarm-restrain-table all** command output

Item	Description
Interface	Interface that functions as an access point.
alarm time	Date and time when alarms were generated.
Total: *m*	Total number of suppressed entries *m*.

13.7.20 local-authorize

Function

The **local-authorize** command specifies the user authorization information to be delivered to an authentication control device.

The **undo local-authorize** command restores the default user authorization information to be delivered to an authentication control device.

By default, all user authorization information can be delivered to an authentication control device.

Format

local-authorize { **none** | { **acl** | **car** | **priority** | **ucl-group** | **vlan** } * }

undo local-authorize

Parameters

Parameter	Description	Value
acl	Delivers ACL authorization information.	-
car	Delivers CAR authorization information.	-
priority	Delivers priority authorization information.	-
ucl-group	Delivers UCL group authorization information. **NOTE** When you authorize the ACL or UCL group, configure the corresponding ACL or UCL group on authentication control devices to ensure that the authorization information takes effect on the authentication control devices.	-
vlan	Delivers VLAN authorization information.	-

Parameter	Description	Value
none	Delivers no authorization information, including: • ACL-based authorization information • CAR-based authorization information • Priority-based authorization information • UCL-based authorization information • VLAN-based authorization information	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable an authentication control device to implement specified user access policies, you can run this command to specify user authorization information to be delivered to the authentication control device. By default, all authorization information is delivered to an authentication control device.

Precautions

This command is supported only on authentication control devices.

This command takes effect for all user authorization types, such as local authorization, remote authorization, and RADIUS dynamic authorization.

For VLAN authorization in a policy association scenario, VLAN authorization information must be delivered. You must configure the **local-authorize vlan** command or do not configure the **local-authorize** command, that is, use the default settings. By default, all user authorization information can be delivered to an authentication control device.

Example

Deliver only UCL group authorization information to the authentication control device.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] local-authorize ucl-group
```

13.7.21 remote-authorize

Function

The **remote-authorize** command specifies the user authorization information to be delivered to an authentication access device.

The **undo remote-authorize** command restores the default user authorization information to be delivered to an authentication access device.

By default, all user authorization information cannot be delivered to authentication access devices.

Format

remote-authorize { **acl** | **car** | **ucl-group** } *

undo remote-authorize

Parameters

Parameter	Description	Value
acl	Delivers ACL authorization information.	-
car	Delivers CAR authorization information.	-
ucl-group	Delivers UCL group authorization information. **NOTE** When you authorize the ACL or UCL group, configure the corresponding ACL or UCL group on authentication access devices to ensure that the authorization information takes effect on the authentication access devices.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable an authentication access device to implement specified user access policies, you can run this command to specify user authorization information to be delivered to the authentication access device. By default, no authorization information is delivered to the authentication access device.

Precautions

This command is supported only on authentication access devices.

This command takes effect for all user authorization information, including local authorization, remote authorization, and RADIUS dynamic authorization information.

In SVF centralized configuration mode, authentication access devices do not support ACL-based authorization or UCL groups.

Example

Deliver only ACL authorization information to the authentication access device.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] remote-authorize acl
```

13.7.22 user-detect

Function

The **user-detect** command enables the online user detection function on an authentication access device.

The **undo user-detect** command disables the online user detection function on an authentication access device.

By default, the online user detection function is enabled on an authentication access device, the detection interval is 100 seconds, and the number of packet retransmission attempts is 3.

Format

user-detect { **interval** *interval-value* | **retry** *retry-value* } *

undo user-detect

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the detection interval.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 100.
retry *retry-value*	Specifies the number of packet retransmission attempts.	The value is an integer that ranges from 1 to 255. The default value is 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user goes offline due to a power failure or network interruption, the authentication access device and authentication control device may still store information about this user, which results in a heavy load on the authentication control device. In addition, a limited number of users can access the device. If a user goes offline unexpectedly but the device still stores information of this user, other users cannot access the network.

After the detection interval is set, the device considers a user to be offline if the user does not respond within the interval. Then the authentication access device and authentication control device delete the saved information about the user, ensuring effective resource usage.

Precautions

This command is supported only on authentication access devices.

You are advised to keep this function enabled on authentication access devices.

This function takes effect only for users who go online after it is configured.

Example

Enable online user detection in the system view, and set the detection interval to 10 seconds and number of packet retransmission attempts to 5.

```
<HUAWEI> system-view
[HUAWEI] user-detect interval 10 retry 5
```


13.7.23 user-sync (authentication access device)

Function

The **user-sync** command enables the user synchronization function on an authentication access device.

The **undo user-sync** command disables the user synchronization function on an authentication access device.

By default, user synchronization is enabled on an authentication access device and the synchronization interval is 60 seconds.

Format

user-sync interval *interval-value*

undo user-sync

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the user synchronization interval.	The value is an integer that ranges from 60 to 3600, in seconds. The default value is 60.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user is disconnected from an authentication access device due to online detection or a failure to send a disconnection request message, the user information on the authentication control device and authentication access device cannot be synchronized.

After the user synchronization interval is reached, the authentication access device sends a synchronization message containing MAC addresses of all online users to the authentication control device. After receiving the synchronization message, the authentication control device responds with a synchronization failure message if it finds that some users are offline. The authentication access device forcibly disconnects the corresponding users according to the synchronization failure message.

Precautions

This command is supported only on authentication access devices.

The user synchronization function needs to be enabled on both authentication access devices and authentication control devices to ensure that the function works properly. In addition, the user synchronization interval configured on authentication access devices must be shorter than or equal to that configured on authentication control devices, preventing users from being disconnected due to incorrect synchronization.

The user synchronization function of authentication access devices depends on whether the control tunnel is available. When the control tunnel is faulty, the user synchronization function becomes abnormal.

Example

Set the user synchronization interval to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] user-sync interval 100
```

13.7.24 user-sync (authentication control device)

Function

The **user-sync** command enables the user synchronization function on an authentication control device.

The **undo user-sync** command disables the user synchronization function on an authentication control device.

By default, user synchronization is enabled on an authentication control device, the synchronization interval is 60 seconds, and the number of synchronization attempts is 10.

Format

user-sync { **interval** *interval-value* | **retry** *retry-value* } *

undo user-sync

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the user synchronization interval.	The value is an integer that ranges from 60 to 3600, in seconds. The default value is 60.
retry *retry-value*	Specifies the maximum number of synchronization attempts.	The value is an integer that ranges from 5 to 300. The default value is 10.

Views

VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user is disconnected from an authentication access device due to online detection or a failure to send a disconnection request message, the user information on the authentication control device and authentication access device cannot be synchronized.

After the user synchronization interval is reached, the number of synchronization attempts is added by 1. If the number of synchronization attempts reaches the maximum, the user is forced offline. If the authentication access device detects that the user is online by sending a synchronization message, the number of synchronization attempts is set to 0.

Precautions

This command is supported only on authentication control devices.

The user synchronization function needs to be enabled on both authentication access devices and authentication control devices to ensure that the function works properly. In addition, the user synchronization interval configured on authentication access devices must be shorter than or equal to that configured on authentication control devices, preventing users from being disconnected due to incorrect synchronization.

Example

Set the user synchronization interval to 100 seconds and maximum number of synchronization attempts to 15 on GE0/0/1 of the authentication control device.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] user-sync interval 100 retry 15
```

13.8 Kerberos Snooping Configuration Commands

13.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.8.2 display kerberos-snooping-profile

Function

The **display kerberos-snooping-profile** command displays the configuration of a Kerberos snooping profile.

Format

display kerberos-snooping-profile [**name** *profile-name*]

Parameters

Parameter	Description	Value
name *profile-name*	Displays the configuration of a specified Kerberos snooping profile. If this parameter is not specified, all Kerberos snooping profiles configured on the device are displayed. If this parameter is specified, the detailed configuration of the specified Kerberos snooping profile is displayed.	The value must be the name of an existing Kerberos snooping profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a Kerberos snooping profile is configured, you can run this command to check whether the configuration of the Kerberos snooping profile is correct.

Example

Display the configuration of all Kerberos snooping profiles configured on the device.

```
<HUAWEI> display kerberos-snooping-profile
----------------------------------------------
```



```
ID          Profile Name
-----------------------------------------------
0           p1
1           p2
-----------------------------------------------
Total: 2 printed: 2.
```

Display the configuration of the Kerberos snooping profile **p1**.

```
<HUAWEI> display kerberos-snooping-profile name p1
 Profile Name              : p1
 TCP/UDP Port              : 99
 Server IP                 : 10.1.1.1
```

Table 13-127 Description of the **display kerberos-snooping-profile** command output

Item	Description
ID	ID of a Kerberos snooping profile.
Profile Name	Name of a Kerberos snooping profile. To configure a Kerberos snooping profile, run the **kerberos-snooping-profile** command in the system view.
Total	Number of Kerberos snooping profiles.
printed	Number of displayed Kerberos snooping profiles.
TCP/UDP Port	Port number of a Kerberos server. To configure the port number of a Kerberos server, run the **port** command in the Kerberos snooping profile view.
Server IP	IP address of a Kerberos server. To configure the IP address of a Kerberos server, run the **server-ip** command in the Kerberos snooping profile view.

13.8.3 display access-user access-type kerberos-snooping

Function

The **display access-user access-type kerberos-snooping** command displays information about online Kerberos users.

Format

display access-user access-type kerberos-snooping

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about online Kerberos users.

Example

Display information about online Kerberos users.

```
<HUAWEI> display access-user access-type kerberos-snooping
--------------------------------------------------------------------------------
UserID Username              IP address      MAC            Status
--------------------------------------------------------------------------------
16018  test                  10.1.1.2        00e0-fc12-3456 Success
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 13-128 Description of the **display access-user access-type kerberos-snooping** command output

Item	Description
UserID	ID that is assigned to a user after the user goes online.
Username	User name.
IP address	User IP address.
MAC	User MAC address.
Status	User status. ● Success: User authentication is successful.
Total	Number of users.
printed	Number of users displayed in the command output.

13.8.4 kerberos-snooping-profile (authentication profile view)

Function

The **kerberos-snooping-profile** command binds a Kerberos snooping profile to an authentication profile.

The **undo kerberos-snooping-profile** command unbinds a Kerberos snooping profile from an authentication profile.

By default, no Kerberos snooping profile is bound to an authentication profile.

Format

kerberos-snooping-profile *profile-name*

undo kerberos-snooping-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a Kerberos snooping profile.	The value must be the name of an existing Kerberos snooping profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After a Kerberos snooping profile is bound to an authentication profile, Kerberos snooping is enabled on the interface to which the authentication profile is applied. The interface then can control network access rights of users.

Prerequisites

A Kerberos snooping profile has been created using the **kerberos-snooping-profile** command in the system view.

Follow-up Procedure

Run the **authentication-profile** command in the interface view and VAP profile view to apply the authentication profile to a Layer 2 physical interface.

Precautions

An authentication profile can have only one Kerberos snooping profile bound.

Example

Bind the Kerberos snooping profile **profile1** to the authentication profile **authen1**.

```
<HUAWEI> system-view
[HUAWEI] kerberos-snooping-profile name profile1
[HUAWEI-krb-snooping-profile-profile1] quit
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] kerberos-snooping-profile profile1
```

13.8.5 kerberos-snooping-profile (system view)

Function

The **kerberos-snooping-profile** command creates a Kerberos snooping profile and displays the Kerberos snooping profile view.

The **undo kerberos-snooping-profile** command deletes a Kerberos snooping profile.

By default, no Kerberos snooping profile is created.

Format

kerberos-snooping-profile name *profile-name*

undo kerberos-snooping-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Kerberos snooping profile.	The value is a string of 1 to 31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following special characters: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In a Kerberos authentication scenario, you need to enable Kerberos snooping on the device, so that the device can control network access rights of users. Only

authenticated users can access network resources. To achieve this, you need to create a Kerberos snooping profile on the device and set parameters in the profile first.

Example

Create a Kerberos snooping profile named **profile1**.

```
<HUAWEI> system-view
[HUAWEI] kerberos-snooping-profile name profile1
[HUAWEI-krb-snooping-profile-profile1]
```

13.8.6 port (Kerberos snooping profile view)

Function

The **port** command configures the port number used by a Kerberos server to send packets.

The **undo port** command restores the default configuration.

By default, a Kerberos server uses port 88 to send packets.

Format

port *port-number*

undo port

Parameters

Parameter	Description	Value
port-number	Specifies the port number used by a Kerberos server to send packets.	The value is an integer in the range from 1 to 65535.

Views

Kerberos snooping profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring Kerberos snooping, you need to run the **port** command to configure the port number used by a Kerberos server to send packets. The device identifies the Kerberos packets sent by a Kerberos server based on the configured IP address and port number of the Kerberos server. If the device receives a KRB_AS_REP, KRB_TGS_REP, or KRB_AP_REP packet from the Kerberos server, it

considers that the user has been authenticated and allows the user to access network resources.

In addition, the device identifies and allows the Kerberos packets sent by clients to pass through if the destination port number of packets is the port number of a Kerberos server.

Precautions

Ensure that the port number configured on the device is the same as that used by the Kerberos server.

Example

Set the port number used by the Kerberos server to send packets to 10000.

```
<HUAWEI> system-view
[HUAWEI] kerberos-snooping-profile name profile1
[HUAWEI-krb-snooping-profile-profile1] port 10000
```

13.8.7 server-ip (Kerberos snooping profile view)

Function

The **server-ip** command configures the IP address of a Kerberos server.

The **undo server-ip** command deletes the configuration of the Kerberos server IP address.

By default, no Kerberos server IP address is configured on the device.

Format

server-ip *server-ip-address* &<1-10>

undo server-ip { *server-ip-address* | **all** }

Parameters

Parameter	Description	Value
server-ip-address	Specifies the IP address of a Kerberos server.	The value is in dotted decimal format.
all	Deletes all Kerberos server IP addresses.	-

Views

Kerberos snooping profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring Kerberos snooping, you need to run the **server-ip** command to configure the IP address of a Kerberos server. The device identifies the Kerberos packets sent by a Kerberos server based on the configured IP address and port number of the Kerberos server. If the device receives a KRB_AS_REP, KRB_TGS_REP, or KRB_AP_REP packet from the Kerberos server, it considers that the user has been authenticated and allows the user to access network resources.

Precautions

Ensure that the IP address configured on the device is the same as that used by the Kerberos server.

Example

Configure the Kerberos server IP address 10.1.1.1 on the device.

```
<HUAWEI> system-view
[HUAWEI] kerberos-snooping-profile name profile1
[HUAWEI-krb-snooping-profile-profile1] server-ip 10.1.1.1
```

