19 Security Commands

About This Chapter

19.1 AAA Configuration Commands
19.2 RADIUS Configuration Commands
19.3 HWTACACS Configuration Commands
19.4 HACA Configuration Commands
19.5 DAA Configuration Commands
19.6 NAC Configuration Commands
19.7 ACL Configuration Commands
19.8 Firewall Configuration Commands
19.9 Deep Security Configuration Commands
19.10 Local Attack Defense Configuration Commands
19.11 Attack Defense Configuration Commands
19.12 Traffic Suppression Configuration Commands
19.13 ARP Security Configuration Commands
19.14 DHCP Snooping Configuration Commands
19.15 IP Source Guard Configuration Commands
19.16 URPF Configuration Commands
19.17 PKI Configuration Commands
19.18 SSL Configuration Commands
19.19 HTTPS Configuration Commands
19.20 Keychain Configuration Commands

 Copyright © Huawei Technologies Co., Ltd.

19.1 AAA Configuration Commands

19.1.1 aaa

Function

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

The **undo aaa** command disables the AAA services.

Format

aaa

undo 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

After you run the **undo aaa** command, the AAA services are disabled. If the domain or service scheme configured for AAA is referenced by other modules, this domain or service scheme is not deleted, but the domain state turns to initialized. A domain in initialized state only binds to the default authentication scheme and accounting scheme, but does not bind to the authorization scheme, RADIUS server, and HWTACACS server. This command does not force online users to log out. You can run the **cut access-user** command to force users to log out.

Example

Access the AAA view.

 Copyright © Huawei Technologies Co., Ltd.

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

19.1.2 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

2: Configuration 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
```

 Copyright © Huawei Technologies Co., Ltd.

19.1.3 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

2: Configuration 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
```

19.1.4 aaa online-fail-record

Function

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

 Copyright © Huawei Technologies Co., Ltd.

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

2: Configuration 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
```

19.1.5 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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

Related Topics

19.1.6 aaa-author-bypass

19.1.7 aaa-author-cmd-bypass

19.1.6 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.5 aaa-authen-bypass

19.1.7 aaa-author-cmd-bypass

19.1.7 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.5 aaa-authen-bypass

19.1.6 aaa-author-bypass

19.1.8 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.

 Copyright © Huawei Technologies Co., Ltd.

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.
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 **19.1.57 local-aaa-user wrong-password** or **19.1.78 remote-aaa-user 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.34 display aaa-quiet administrator except-list

19.1.9 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-aaa] accounting-scheme scheme1
[Huawei-aaa-accounting-scheme1] accounting realtime 3
[Huawei-aaa-accounting-scheme1] accounting interim-fail max-times 5 offline
```

Related Topics

19.1.10 accounting realtime

19.1.10 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

 Copyright © Huawei Technologies Co., Ltd.

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 19-1 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
```

Related Topics

19.1.9 accounting interim-fail

 Copyright © Huawei Technologies Co., Ltd.

19.1.11 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.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The command takes effect only when the accounting mode configured using the **19.1.13 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
```

19.1.12 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 value must be an existing RADIUS server template name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

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 must be 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 **huawei** domain, set the IP addresses of the RADIUS authentication and accounting servers to 10.1.1.1, port IDs of the servers to 1813 and 1814, name of the RADIUS server template to which the RADIUS authentication and accounting servers belong to **t1**, IP address of the level-2 RADIUS accounting server to 10.1.1.2, port ID of the server to 1814, and name of the RADIUS server template to which the level-2 RADIUS accounting server belongs 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 huawei
[Huawei-aaa-domain-huawei] radius-server t1
[Huawei-aaa-domain-huawei] accounting-copy radius-server t2
```

19.1.13 accounting-mode

Function

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

 Copyright © Huawei Technologies Co., Ltd.

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.	-
haca	Indicates that accounting is performed by an HACA server.	-

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 or HACA. 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

 Copyright © Huawei Technologies Co., Ltd.

The device does not support local accounting. When the authentication scheme configured using the **19.1.19 authentication-mode (authentication scheme view)** command defines local authentication, you need to run the **accounting-mode none** command to configure non-accounting or run the **19.1.11 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 **19.1.50 domain (AAA view)** command.

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
```

19.1.14 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.1.15 accounting-scheme (AAA view)** 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
```

Related Topics

19.1.15 accounting-scheme (AAA view)

19.1.38 display accounting-scheme

19.1.15 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*

 Copyright © Huawei Technologies Co., Ltd.

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 **19.1.14 accounting-scheme (AAA domain view)** 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

 Copyright © Huawei Technologies Co., Ltd.

accounting-scheme command in the AAA view displays the accounting scheme view directly.

The system supports a maximum of 32 accounting schemes, including the default accounting scheme.

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]
```

Related Topics

19.1.14 accounting-scheme (AAA domain view)

19.1.16 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 level.

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

By default, the user level is not configured.

Format

admin-user privilege level *level*

undo admin-user privilege level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
level	Specifies the level of a user. A larger value indicates a higher user level. After logging in to the device, a user can run only the commands of the same level or lower 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 level, and a user can run only the commands of the same level or lower levels. By using the **admin-user privilege level** command to set the user level, the device controls commands used by users.

By default, commands are classified into the following 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 Telnet 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 refinedly, upgrade command levels to levels 0 to 15. You can run the **command-privilege level** command to upgrade command levels in a batch.

- If non-authentication is used, the administrator level is specified using the **user privilege** command in the VTY interface view.

 Copyright © Huawei Technologies Co., Ltd.

- If local authentication is used, the administrator level is specified using the **local-user privilege level** command.
- If remote authentication is used, the administrator level can be set in the following ways, in descending order of priority:
  a. Using the user 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 level in a service scheme
  c. Running the **user privilege** command to set the user level in the VTY interface view
- If remote authentication and local authentication are configured, remote authentication is first used. If remote authentication fails, local authentication is used. The administrator level can be set in the following ways, in descending order of priority:
  a. Using the user level sent by an authentication server to the device after authentication has succeeded
  b. Running the **local-user privilege level** command to set the local user level

  NOTE

  The local user level is used only when the remote authentication server is faulty. If the remote authentication server responds to authentication requests but does not deliver user levels, the configured local user level does not take effect.

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 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 level in a service scheme.

Example

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

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

Related Topics

19.1.47 display service-scheme

19.1.60 local-user

19.1.90 service-scheme (AAA view)

3.8.24 user privilege

 Copyright © Huawei Technologies Co., Ltd.

19.1.17 authentication { roam-accounting | update-ip-accounting } * enable

Function

The **authentication** { **roam-accounting** | **update-ip-accounting** } * **enable** command enables a device to send accounting packets for roaming and address updating.

The **undo authentication** { **roam-accounting** | **update-ip-accounting** } * **enable** command disables a device from sending accounting packets for roaming and address updating.

By default, the device is enabled to send accounting packets for roaming and address updating.

Format

authentication { **roam-accounting** | **update-ip-accounting** } * **enable**

undo authentication { **roam-accounting** | **update-ip-accounting** } * **enable**

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

By default, the device sends accounting packets for roaming 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-ip-accounting** } * **enable** command to disable the device from sending accounting packets for roaming and address updating, saving resources on the device. After roaming and address updating are complete, the device sends accounting packets again and the accounting function is not affected.

- **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 address updating.
- If the terminal information (including the DHCP Option, UA, or LLDP information) is updated for the first time, the device immediately triggers

 Copyright © Huawei Technologies Co., Ltd.

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-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
```

19.1.18 authentication roam-accounting update-session-mode

Function

The **authentication roam-accounting update-session-mode** command enables the accounting session update mode during roaming accounting.

The **undo authentication roam-accounting update-session-mode** command disables the accounting session update mode during roaming accounting.

By default, the accounting session update mode is not used during roaming accounting.

Format

authentication roam-accounting update-session-mode

undo authentication roam-accounting update-session-mode

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For multi-link accounting users, each link corresponds to different values of the RADIUS attribute Acct-Session-Id, but all links correspond to the same value of the RADIUS attribute Acct-Multi-Session-Id. After the roaming accounting function is enabled for users using the **authentication roam-accounting enable** command,

 Copyright © Huawei Technologies Co., Ltd.

users' accounting session IDs are carried in the RADIUS attribute Acct-Session-Id. However, if the Acct-Session-Id changes, the server performs accounting again. To resolve this problem, you can run the **authentication roam-accounting update-session-mode** command to configure the accounting session update mode during roaming accounting. After this command is configured, user accounting packets carry the RADIUS attribute Acct-Multi-Session-Id. During roaming accounting, the RADIUS attribute Acct-Multi-Session-Id is used to identify users.

Precautions

This function takes effect only after the roaming accounting function is enabled for users using the **authentication roam-accounting enable** command.

Example

Enables the accounting session update mode during roaming accounting.

```
<Huawei> system-view
[Huawei] authentication-profile name test
[Huawei-authentication-profile-test] authentication roam-accounting update-session-mode
```

19.1.19 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.

Format

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

authentication-mode none

undo authentication-mode

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.	-
radius	Authenticates users using a RADIUS server. To perform RADIUS authentication, configure a RADIUS authentication server in a RADIUS server template.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.

 Copyright © Huawei Technologies Co., Ltd.

- 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.

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.

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
```

19.1.20 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.21 authentication-scheme (AAA view)

19.1.39 display authentication-scheme

19.1.21 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:

 Copyright © Huawei Technologies Co., Ltd.

- 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

 Copyright © Huawei Technologies Co., Ltd.

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]
```

Related Topics

19.1.20 authentication-scheme (AAA domain view)

19.1.39 display authentication-scheme

19.1.22 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** | **super** } * [**none**]

authentication-super none

undo authentication-super

Parameters

Parameter	Description	Value
hwtacacs	Uses HWTACACS authentication to upgrade user levels.	-
super	Uses local authentication to upgrade user levels.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 **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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

3.8.3 authentication-mode (user interface view)
19.1.20 authentication-scheme (AAA domain view)
19.1.21 authentication-scheme (AAA view)
19.1.39 display authentication-scheme

19.1.23 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 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 level.

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

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After being authorized, the users at a certain level can run the commands of the same or lower 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 level, the commands run by the users at that 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.

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 level cannot run any commands except for the **quit** command. The administrator needs to log in again.

Example

Configure command line authorization administrators at level 2.

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

19.1.24 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.

Format

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

 Copyright © Huawei Technologies Co., Ltd.

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 (authentication exemption excluded) is authorized. The configuration of if-authenticated authorization does not take effect in RADIUS authentication.	-
local	Authenticates users locally	-
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

 Copyright © Huawei Technologies Co., Ltd.

- 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.
- When the authorization mode is **if-authenticated** or **none**, the user privilege level is inherited from the user domain or is the same as that set in the VTY user view.
- 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.

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
```

19.1.25 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

NOTE

The modify mode is valid for only the user authorization information, such as ACL rule and dynamic VLAN.

Parameters

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

 Copyright © Huawei Technologies Co., Ltd.

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 service 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.1.26 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.27 authorization-scheme (AAA view)

19.1.40 display authorization-scheme

19.1.27 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 --.

 Copyright © Huawei Technologies Co., Ltd.

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.

The system supports a maximum of 32 authorization schemes, including the default authorization scheme.

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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[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]
```

Related Topics

19.1.26 authorization-scheme (AAA domain view)

19.1.28 auto-update url (service scheme view)

Function

The **auto-update url** command configures the URL and version number of a service scheme.

The **undo auto-update url** command deletes the URL and version number of a service scheme.

By default, the URL and version number of a service scheme are not configured.

Format

auto-update url *url-string* **version** *version-number*

undo auto-update url

Parameters

Parameter	Description	Value
url-string	Indicates the URL.	The value is a string of 1 to 208 case-sensitive characters.
version-number	Indicates the version number.	The value is an integer that ranges from 1 to 4294967294.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

The AAA service scheme allows the URL and version number to be bound. IPSec binds the AAA service scheme to the IPSec policy template and sends the URL and version number to users.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the URL **ftp://huawei:huawei2012@10.10.10.1/test** and version number **1** for the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] auto-update url ftp://huawei:huawei2012@10.10.10.1/test version 1
```

Related Topics

19.1.47 display service-scheme

19.1.29 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.45 display recording-scheme

19.1.76 recording-mode hwtacacs

19.1.77 recording-scheme

19.1.30 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* | **ssid** *ssid-name* | **user-group** *group-number* | **user-id** *begin-number* [*end-number*] | **username** *user-name* }

cut access-user access-type { **admin** [**ftp** | **ssh** | **telnet** | **terminal** | **web**] | **ppp** | **l2tp** } [**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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 is a string of 1 to 31 case-sensitive characters without spaces.
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 LPU.	The value range depends on the model of the device.
ssid *ssid-name*	Disconnects sessions initiated by a service set identifier (SSID).	The SSID must already exist.
user-group *group-number*	Disconnects sessions of a user-group.	The value is a string of 1 to 64 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.
user-id *begin-number* [*end-number*]	Disconnects sessions of a specified user.	The user-id must exist on the device.

 Copyright © Huawei Technologies Co., Ltd.

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	-
ppp	Displays information about online users using PPP authentication.	-
l2tp	Displays information about online users using L2TP authentication.	-

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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.37 display access-user (All views)

19.1.31 dhcp-server group (service scheme view)

Function

The **dhcp-server group** command specifies an existing DHCP server group in a service scheme.

The **undo dhcp-server group** command deletes the DHCP server group in a service scheme.

By default, no DHCP server group is specified in a service scheme.

Format

dhcp-server group *group-name*

undo dhcp-server group

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 case-sensitive characters without spaces. The DHCP server group must have been configured using the **dhcp server group** command.

Views

Service scheme view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If a service scheme is bound to a domain, the service scheme configurations are valid for the users in the domain.

Example

Specify the DHCP server group **group1** for the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] dhcp-server group group1
```

Related Topics

8.3.40 dhcp server group

19.1.47 display service-scheme

19.1.32 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
reverse-order	Displays the records in a sequence reverse to the sequence in which they were generated. That is, the latest records are displayed first.	-
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.	-
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 is a string of 1 to 31 characters without spaces. It is case sensitive.
mac-address *mac-address*	Specifies a MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
access-slot *slot-number*	Specifies the slot ID.	The value is an integer. It must be the slot ID of an operating LPU.
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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 (~).

When the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following 19; that is, only 22 characters are displayed.

Example

View information about user normal logouts in domain **rds**.

```
<Huawei> display aaa offline-record domain rds
 ------------------------------------------------------------------------
  User name             : test@rds
  Domain name             : rds
  User MAC              : 0021-9746-b67c
  User access type      : 802.1x
  User access interface : GigabitEthernet1/0/2
  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                 : 1
  Radio ID              : 0
  AP MAC                  : b001-0000-ac01
  SSID                  : ssid1
```

 Copyright © Huawei Technologies Co., Ltd.

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

Table 19-2 Description of the **display aaa offline-record domain** command output

Item	Description
User name	User name.
Domain name	Domain of a user.
User 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. • PPPoE indicates that the user accesses the network through PPPoE. • 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. • Bind indicates that the user accesses the network through IP session. • SSLVPN indicates that the user accesses the network through SSL VPN. For the related command, see **19.1.67 local-user service-type**.
User access interface	Access interface of a user.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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	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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
User offline 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 an STA is disassociated. ● 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 "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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• The value "Accounting server no response" indicates that the accounting server does not respond. • The value "Local Authentication user block" indicates that the local user is locked. • The value "Authorize vlan error" indicates that VLAN authorization fails.
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.

19.1.33 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

 Copyright © Huawei Technologies Co., Ltd.

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: 256     used: 3
 Authentication-scheme            : total: 33      used: 1
 Accounting-scheme                : total: 32      used: 2
 Authorization-scheme             : total: 32      used: 1
 Service-scheme                 : total: 256     used: 1
 Recording-scheme                 : total: 32      used: 0
 Local-user                     : total: 512     used: 10
 Local-user block retry-interval  : 30 Min(s)
 Local-user block retry-time      : 5
 Local-user block time            : 30 Min(s)
 Remote-user block retry-interval : 5 Min(s)
 Remote-user block retry-time     : 3
 Remote-user block time           : 5 Min(s)
 Session timeout invalid enable   : Yes
```

Table 19-3 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 @.
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 user name and domain name. • Left to right • Right to left
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.
Local-user block retry-time	Maximum number of consecutive authentication failures.
Local-user block time	Locking time of a local account.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remote-user block retry-interval	Authentication retry interval of a remote AAA authentication user.
Remote-user block retry-time	Maximum number of consecutive authentication failures.
Remote-user block time	Locking time of a remote AAA authentication user.
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.

Related Topics

19.1.1 aaa
19.1.50 domain (AAA view)

19.1.34 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 **19.1.8 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.

 Copyright © Huawei Technologies Co., Ltd.

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 19-4 Description of the **display aaa-quiet administrator except-list** command output

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

19.1.35 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.

 Copyright © Huawei Technologies Co., Ltd.

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 19-5 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.

19.1.36 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.

 Copyright © Huawei Technologies Co., Ltd.

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 19-6 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 **19.1.30 cut access-user** command.

19.1.37 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* | **user-group** *user-group-name* | **username** *user-name*] [**detail**]

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

display access-user statistics

display access-user access-type { **admin** [**ftp** | **ssh** | **telnet** | **terminal** | **web**] | **ppp** | **l2tp** } [**username** *user-name*]

Parameters

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

 Copyright © Huawei Technologies Co., Ltd.

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.	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** When the user type is NAC, details about the user are displayed. When the user is in another type, brief information about the user 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 VPN instance must already exist.
ipv6-address *ipv6-address*	Displays information about the user with a specified IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers 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.
service-scheme *service-scheme-name*	Displays information about the user with a specified service scheme.	The service scheme must already exist.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
access-slot *slot-id*	Displays information about users connecting to a specified LPU.	The value range depends on the model of the device.
ssid *ssid-name*	Specifies the SSID.	The SSID must already exist.
statistics	Displays user statistics on the device. • Historical user statistics: displays historical WLAN user statistics on the device. • Current online user statistics: displays current user statistics on the device.	-
user-group *user-group-name*	Displays information about users in a specified user group.	The value is a string of 1 to 64 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.
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.
username *user-name*	Displays information about the user with a user name.	The user name must already exist.
detail	Displays detailed information about users.	-
access-type	Displays information about the users using the specified authentication mode.	-

 Copyright © Huawei Technologies Co., Ltd.

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	-
ppp	Displays information about online users using PPP authentication.	-
l2tp	Displays information about online users using L2TP authentication.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays information about user sessions on the device.

Precautions

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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following 19; that is, only 22 characters are displayed.

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

Example

Display the users connected to the interface Eth2/0/0.

```
<Huawei> display access-user interface ethernet 2/0/0
------------------------------------------------------------------------------------------------
UserID Username                  IP address              MAC            Status
------------------------------------------------------------------------------------------------
36     test@rds                  -                       0021-9746-b67c  Success
17     c0a80642@none             192.168.6.66            4487-fc40-f05b  Success
------------------------------------------------------------------------------------------------
Total 2,2 printed
```

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 the user with the user ID being 36.

```
<Huawei> display access-user user-id 36

Basic:
  User ID                     : 36
  User name                   : test@rds
  Domain-name                 : rds
  User MAC                    : 0021-9746-b67c
  User IP address             : -
  User IPv6 address           : -
  User access Interface       : Ethernet2/0/0
  QinQVlan/UserVlan           : 0/10
  User access time            : 2010/11/28 23:37:27
  User accounting session ID  : Huawei04007000000010d****3000036
  User access type            : 802.1x
  User Privilege              : 15
  Terminal Device Type        : Data Terminal
  Dynamic ACL ID(Effective)   : 3100
  Dynamic group index(Effective) : 10
  Dynamic group name(Effective)  : nac
  Upstream CAR CIR            : 300
  Upstream CAR PIR            : 200
  Upstream CAR CBS            : 56400
  Upstream CAR PBS            : 37600
  Up packets number(Packet)   : 239
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Up bytes number(Byte)          : 19,171
  Downstream CAR CIR             : 500
  Downstream CAR PIR             : 400
  Downstream CAR CBS             : 94000
  Downstream CAR PBS             : 75200
  Down packets number(Packet)    : 4
  Down bytes number(Byte)        : 256

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 being 17.

```
<Huawei> display access-user user-id 17

Basic:
  User ID                    : 17
  User name                  : c0a80642
  Domain-name                : none
  User MAC                   : 4487-fc40-f05b
  User IP address            : 192.168.6.66
  User IPv6 address          : -
  User access Interface      : Ethernet2/0/0
  QinQVlan/UserVlan          : 0/6
  User access time           : 2014/09/10 13:15:39
  User accounting session ID : Huawei04007000000010d****3000036
  User access type           : WEB
  User Privilege             : 15
  AP ID                      : 0
  AP name                    : ap-0
  Radio ID                   : 0
  AP MAC                     : 0a0b-0c00-0500
  SSID                       : 222222
  Online time                : 417(s)
  Web-server IP address      : 10.9.9.1
  User session timeout       : 4(h)

AAA:
  User authentication type       : WEB authentication
  Current authentication method  : None
  Current authorization method   : -
  Current accounting method      : None
```

Display user statistics on the device.

```
<Huawei> display access-user statistics
Historical wireless user statistics:
 Access total number        : 358
 Access failed number       : 0
 Access success number      : 358
 Abnormal offline number    : 0
Current online user statistics:
  Total access number           : 0
  MAC access number             : 0
  802.1x access number          : 0
  Web access number             : 0
  Static access number          : 0
  PPPoE access number           : 0
  Unauthenticated access number : 0
```

Table 19-7 Description of the **display access-user** command output

Item	Description
Basic	Basic information about a user.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
User ID	ID of a user.
User name	Name of a user.
Domain-name	Name of the domain that a user belongs to.
User MAC	MAC address of a user.
User IP address	IP address of a user.
User IPv6 address	IPv6 address of a user.
User access Interface	Access interface connected to a user.
Status	Whether a user joins a VLAN. • Open: no authentication • 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
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 access time	Time when a user goes online.
User accounting session ID	ID of the accounting session for a user.
User access type	Access type of a user.
User Privilege	Level of a user.
Terminal Device Type	Terminal device type of a user.
Dynamic ACL ID(Effective)	ACL ID. • Effective: The dynamic ACL has taken effect. • Effective: The dynamic ACL has taken effect.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
Upstream CAR CIR	Upstream CIR dynamically delivered by the RADIUS server to online user.
Upstream CAR PIR	Upstream PIR dynamically delivered by the RADIUS server to online user.
Upstream CAR CBS	Upstream CBS dynamically delivered by the RADIUS server to online user.
Upstream CAR PBS	Upstream PBS dynamically delivered by the RADIUS server to online user.
Up packets number(Packet)	Number of incoming packets of a user.
Up bytes number(Byte)	Number of bytes in incoming packets of a user.
Downstream CAR CIR	Downstream CIR dynamically delivered by the RADIUS server to online user.
Downstream CAR PIR	Downstream PIR dynamically delivered by the RADIUS server to online user.
Downstream CAR CBS	Downstream CBS dynamically delivered by the RADIUS server to online user.
Downstream CAR PBS	Downstream PBS dynamically delivered by the RADIUS server to online user.
Down packets number(Packet)	Number of outgoing packets of a user.
Down bytes number(Byte)	Number of bytes in outgoing packets of a user.
Web-server IP address	IP address of the WEB server.
User session timeout	Timeout interval of user sessions.
AP ID	ID of the AP connected to users.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Online time	STA online time.
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 mode.
Current authorization method	Authorization mode.
Current accounting method	Accounting mode.
Historical user statistics	Number of history users.
Access total number	Total access times users.
Access failed number	Number of times users fail to access.
Access success number	Number of times users successfully access.
Abnormal offline number	Number of times users go offline unexpectedly.
Current online user statistics	Number of online users.
Total access number	Total number of access users.
MAC access number	Number of online users passing MAC address authentication.
802.1x access number	Number of online users passing 802.1X authentication.
Web access number	Number of online users passing web authentication.
Static access number	Number of online static users.
PPPoE access number	Number of online PPPoE users.
Unauthenticated access number	Number of users failing authentication.

19.1.38 display accounting-scheme

Function

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

 Copyright © Huawei Technologies Co., Ltd.

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 already 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 view the configuration of accounting schemes.

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

The **display accounting-scheme** command displays the detailed configuration if the name of an accounting scheme is specified. 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
  ------------------------------------------------------------------------
  default                           None
  radius-1                          RADIUS
  tacas-1                           HWTACACS
  haca-1                            HACA

  ------------------------------------------------------------------------
  Total of accounting-scheme: 4
```

Display the detailed configuration of the default accounting scheme.

```
<Huawei> display accounting-scheme default

  Accounting-scheme-name            : default
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 19-8 Description of the **display accounting-scheme** command output

Item	Description
Accounting-scheme-name	Name of an accounting scheme. To create an accounting scheme, run the **accounting-scheme (AAA view)** command.
Accounting-method	Accounting mode in the accounting scheme. The accounting modes are as follows: • HWTACACS: indicates that an HWTACACS server performs accounting. • None: indicates non-accounting. • RADIUS: indicates that a RADIUS server performs accounting. • HACA: indicates that an HACA server performs accounting. To configure an 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 set the interval for real-time accounting, run the **accounting realtime** command.
Realtime-accounting-interval(min)	Interval for real-time accounting. To set the interval for real-time accounting, run the **accounting realtime** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Start-accounting-fail-policy	Policy used for accounting-start failures. • Offline: disconnects users. • Online: keeps users online. To configure a policy for accounting-start failures, run the **accounting start-fail** command.
Realtime-accounting-fail-policy	Policy used for real-time accounting failures. • Offline: disconnects users. • Online: keeps users online. To configure the policy used for 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 set the number of real-time retries before a real-time accounting failure is confirmed, run the **accounting interim-fail** command.

19.1.39 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 already exist.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the authentication scheme configuration is complete, run the **display authentication-scheme** command to view the configuration of authentication schemes.

Precautions

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

Example

Display the summary of all authentication schemes.

```
<Huawei> display authentication-scheme
  ------------------------------------------------------------------------
  Authentication-scheme-name          Authentication-method
  ------------------------------------------------------------------------
  default                             Local
  radius                              RADIUS
  ------------------------------------------------------------------------
  Total of authentication scheme: 2
```

Display the detailed configuration of the default authentication scheme.

```
<Huawei> display authentication-scheme default

  Authentication-scheme-name          : default
  Authentication-method               : Local
```

Table 19-9 Description of the **display authentication-scheme** command output

Item	Description
Authentication-scheme-name	Name of an authentication scheme. To create an authentication scheme, run the **19.1.21 authentication-scheme (AAA view)** command.
Authentication-method	Authentication mode in an authentication scheme. To configure an authentication mode in an authentication scheme, run the **19.1.19 authentication-mode (authentication scheme view)** command.

Copyright © Huawei Technologies Co., Ltd.

19.1.40 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 already 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 view the configuration of authorization schemes.

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

Precautions

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

Example

Display the summary of all authorization schemes.

```
<Huawei> display authorization-scheme
  ------------------------------------------------------------------
  Authorization-scheme-name        Authorization-method
  ------------------------------------------------------------------
  default                          Local
```

 Copyright © Huawei Technologies Co., Ltd.

```
scheme0                         Local
------------------------------------------------------------------------------
 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 19-10 Description of the **display authorization-scheme** command output

Item	Description
Authorization-scheme-name	Name of the authorization scheme. To create an authorization scheme, run the **authorization-scheme (AAA view)** command.
Authorization-method	Authorization mode set for the authorization scheme. To configure an authorization mode, run the **authorization-mode** command.
Authorization-cmd level	Whether the command line authorization function is enabled for a user with a specified level: • Disabled: indicates that the command line authorization function is disabled. • Enabled: indicates that the command line authorization function is enabled. To set the command line authorization function, run the **authorization-cmd** command.
Authorization-cmd no-response-policy	Policy for command line authorization failures, in which users are allowed to go online.

 Copyright © Huawei Technologies Co., Ltd.

19.1.41 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 name of a domain. 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 by the **domain** command with required parameters specified, 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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-11 Description of the **display domain** command output

Item	Description
index	Index of a domain. To configure this parameter, run the **19.1.50 domain (AAA view)** command.
DomainName	Name of a domain. To configure this parameter, run the **19.1.50 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         : -
 HWTACACS-server-template       : -
 User-group                     : -
 Push-url-address               : -
 Domain auto block Time-range   : asd
 Flow-statistic                 : enable
 Tariff-level
  Qos-profile                   : huawei
  Accounting-flag               : enable
```

Table 19-12 Description of the **display domain name** command output

Item	Description
Domain-name	Name of a domain. To configure this item, run the **19.1.50 domain (AAA view)** command.
Domain-index	Index of a domain. To configure this item, run the **19.1.50 domain (AAA view)** command.
Domain-state	Status of a domain. • Active: indicates that the domain is activated. • Block: indicates that the domain is blocked. To configure this item, run the **19.1.91 state (AAA domain view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication-scheme-name	Name of the authentication scheme used in a domain. To configure this item, run the **19.1.20 authentication-scheme (AAA domain view)** command.
Accounting-scheme-name	Name of the accounting scheme used in a domain. To configure this item, run the **19.1.14 accounting-scheme (AAA domain view)** command.
Authorization-scheme-name	Name of the authorization scheme used in a domain. To configure this item, run the **19.1.26 authorization-scheme (AAA domain view)** command.
Service-scheme-name	Name of the service scheme used in a domain. To configure this item, run the **19.1.89 service-scheme (aaa domain view)** command.
RADIUS-server-template	Name of the RADIUS server template used in a domain. To configure this item, run the **19.2.21 radius-server (aaa domain view)** command.
HWTACACS-server-template	Name of the HWTACACS server template used in a domain. To configure this item, run the **19.3.5 hwtacacs-server** command.
User-group	Name of the user group authorized to users in a domain. To configure this item, run the **19.1.94 user-group (AAA domain view)** command.
Push-url-address	Pushed URL used in a domain. To configure this item, run the **19.6.80 force-push** command.
Domain auto block Time-range	Automatic block time range of a domain.
Flow-statistic	Whether traffic statistics collection is enabled for users in a domain. • enable: The function is enabled. • -: The function is disabled. To configure this item, run the **19.1.92 statistic enable (AAA domain view)** command.
Tariff-level	Tariff level.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Qos-profile	QoS profile corresponding to the tariff level.
Accounting-flag	Whether accounting is enabled for the tariff level. • enable: The function is enabled. • disable: The function is disabled.

19.1.42 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

 Copyright © Huawei Technologies Co., Ltd.

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       : -
 Access-limit        : Yes
 Access-limit-max    : 4294967295
 Accessed-num        : 0
 Idle-timeout        : -
 User-group          : -
 Account-type        : cmcc-tr069
 Original-password   : No
 Password-set-time   : 2019-12-01 18:42:57+01:00 DST
 Password-expired    : No
 Password-expire-time : -
 Account-expire-time  : -
 Bind IP             : 10.1.1.1
```

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 **19.1.57 local-aaa-user wrong-password** command, the user is locked.

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
```

 Copyright © Huawei Technologies Co., Ltd.

```
  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  : -
```

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  : -
```

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  : -
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-13 Description of the **display local-user** command output

Item	Description
User-name	Name of the local user. To configure this parameter, run the **19.1.60 local-user** command.
State	State of the local user: • A: Active • B: Block To configure this parameter, run the **19.1.60 local-user** command.
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. • B: indicates the IP session 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. To configure this parameter, run the **19.1.67 local-user service-type** command.
AdminLevel	Local user level. To configure this parameter, run the **19.1.60 local-user** command.
Password	Password of the local user. To configure this parameter, run the **19.1.60 local-user** command.
Service-type-mask	Service type of the local user. Same as the AuthMask type. To configure this parameter, run the **19.1.67 local-user service-type** command.
Privilege level	Local user level. To configure this parameter, run the **19.1.60 local-user** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ftp-directory	FTP directory of the local user. To configure this parameter, run the **19.1.60 local-user** command.
Access-limit	Whether the maximum number of sessions of the local user is configured. To configure this parameter, run the **19.1.60 local-user** command.
Access-limit-max	Maximum number of sessions of the local user. To configure this parameter, run the **19.1.60 local-user** command.
Accessed-num	Number of established sessions.
Idle-timeout	Idle timeout interval. To configure this parameter, run the **19.1.60 local-user** command.
User-group	Authorization information of the user group to which the local user is bound. To configure this parameter, run the **19.1.60 local-user** command.
Account-type	Account type of the local user. To set the account type of the local user to CMCC-TR069, run the **local-user account-type** command.
Original-password	Whether the password of a local user is the initial password: • Yes • No To configure this parameter, run the **19.1.71 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 **19.1.72 password expire** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **19.1.64 local-user expire-date** command.
Bind IP	IP address bound to a local user. To configure this parameter, run the **19.1.62 local-user bind-ip** command.
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 **19.1.57 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 **19.1.57 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 **19.1.57 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 **19.1.57 local-aaa-user wrong-password** command.

Related Topics

19.1.60 local-user

19.1.43 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

Copyright © Huawei Technologies Co., Ltd.

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 19-14 Description of the **display local-user expire-time** command output

Item	Description
Username	Local account name. To configure this parameter, run the **19.1.60 local-user** command.
Password-expire	Number of days after which the password expires. To configure this parameter, run the **19.1.72 password expire** command.
Account-expire	Account expiration time. To configure this parameter, run the **19.1.64 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.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.1.64 local-user expire-date
19.1.72 password expire

19.1.44 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)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-15 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 **19.1.58 local-aaa-user password policy access-user** 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 **19.1.73 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 19-16 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 **19.1.59 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 **19.1.72 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 **19.1.73 password history record number** command.
Password alert before expiration	Password expiration prompt days. To configure this function, run the **19.1.70 password alert before-expire** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Password alert original	Whether the device prompt users to change the initial passwords: • Enable • Disable To configure this function, run the **19.1.71 password alert original** command.

Related Topics

19.1.58 local-aaa-user password policy access-user
19.1.59 local-aaa-user password policy administrator
19.1.72 password expire
19.1.70 password alert before-expire
19.1.71 password alert original
19.1.73 password history record number

19.1.45 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

Copyright © Huawei Technologies Co., Ltd.

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 19-17 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.
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.

Related Topics

19.1.76 recording-mode hwtacacs

19.1.77 recording-scheme

19.1.46 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*]

 Copyright © Huawei Technologies Co., Ltd.

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

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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display remote-user authen-fail
  Interval: Retry Interval(Mins)
  TimeLeft: Retry Time Left
  BlockDuration: Block Duration(Mins)
  ------------------------------------------------------------------------------
  Username                Interval  TimeLeft  BlockDuration
  ------------------------------------------------------------------------------
  www@test                0         0         65414
  ------------------------------------------------------------------------------
  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
  ------------------------------------------------------------------------------
  www@test                0         0         65414         2018-04-23
17:22:09+08:00
  ------------------------------------------------------------------------------
  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:
  Retry-interval    : 0 Min(s)
  Retry-time-left   : 0
  Block-time-left   : 4 Min(s)
  User-state        : Block
```

Table 19-18 Description of the **display remote-user authen-fail** command output

Item	Description
Username	User name.
Interval: RetryInterval(Mins)	Authentication retry interval, in minutes. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.
Retry-interval	Authentication retry interval. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.
TimeLeft: Retry Time Left	Remaining number of consecutive authentication failures. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.
Retry-time-left	Remaining number of consecutive authentication failures. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
BlockDuration: Block Duration(Mins)	User account locking duration, in minutes. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.
BlockTime	User account locking time.
Block-time-left	Remaining locking time of an account.
User-state	User status: • Block • Active

Related Topics

19.1.78 remote-aaa-user authen-fail

19.1.47 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.

 Copyright © Huawei Technologies Co., Ltd.

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-dns-name       : -
  service-scheme-primary-dns    : -
  service-scheme-secondary-dns  : -
  service-scheme-adminlevel     : 15
  service-scheme-dhcpgroup      : -
  service-scheme-ippool         : -
  service-scheme-primary-wins   : -
  service-scheme-secondary-wins : -
  service-scheme-update-config  : -
  service-scheme-update-version : -
  service-scheme-acl-number     : -
  service-scheme-interface-flag : -
  service-scheme-qosprofile     : -
  service-scheme-idlecut-time   : 10
  service-scheme-idlecut-flow   : 20
  service-scheme-idlecut-direct : Inbound and Outbound
  Tariff-level                  : 1
   Qos-profile                  : svcscheme1000
   Accounting-flag              : enable
```

Table 19-19 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 the service scheme.
service-scheme-dns-name	Default DNS domain name in the service scheme.
service-scheme-primary-dns	Address of the primary DNS server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
service-scheme-secondary-dns	Address of the secondary DNS server.
service-scheme-adminlevel	Level of an administrator. The value is an integer that ranges from 0 to 15. The value 15 indicates that this parameter is invalid. To configure a level of an administrator, run the **admin-user privilege level** command.
service-scheme-dhcpgroup	DHCP server group.
service-scheme-ippool	IP address pool in the service scheme.
service-scheme-primary-wins	Address of the primary wins server.
service-scheme-secondary-wins	Address of the secondary wins server.
service-scheme-update-config	The URL of the update packet.
service-scheme-update-version	Version number of the update packet.
service-scheme-acl-number	The local subnet information to be sent to the remote end.
service-scheme-interface-flag	The address of the interface bound to the IPSec tunnel to be sent to the remote end.
service-scheme-qosprofile	Name of the bound QoS profile. To configure this item, run the **19.1.75 qos-profile (service scheme view)** command.
service-scheme-idlecut-time	Idle-cut timeout interval, in minutes. To configure this item, run the **19.1.55 idle-cut (service scheme view)** command.
service-scheme-idlecut-flow	Traffic threshold for idle-cut, in kbytes. To configure this item, run the **19.1.55 idle-cut (service scheme view)** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
service-scheme-idlecut-direct	Direction in which idle-cut takes effect for traffic. The value can be: • 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 **19.1.55 idle-cut (service scheme view)** command.
Tariff-level	Tariff level of traffic.
Qos-profile	QoS profile corresponding to the tariff level. To set the tariff level, run the **tariff-level** command.
Accounting-flag	Whether accounting is enabled for the tariff level: • enable • disable To enable accounting for the tariff level, run the **tariff-level** command.

Related Topics

19.1.90 service-scheme (AAA view)

19.1.48 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*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

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

Related Topics

19.1.47 display service-scheme

19.1.49 dns-name (service scheme view)

Function

The **dns-name** command configures the default DNS domain name in a service scheme.

The **undo dns-name** command deletes the default DNS domain name in a service scheme.

By default, no default DNS domain name is configured in a service scheme.

 Copyright © Huawei Technologies Co., Ltd.

Format

dns-name *domain-name*

undo dns-name

Parameters

Parameter	Description	Value
domain-name	Specifies the default DNS domain name.	The value is a string of 1 to 255 case-sensitive characters. For example, the value can be **huawei.com**.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

The AAA service scheme allows the default DNS domain name to be bound and sends the default DNS domain name to users.

Example

Configure the default DNS domain name in the service scheme **svcscheme1** to **huawei.com**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] dns-name huawei.com
```

Related Topics

19.1.47 display service-scheme

19.1.50 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*]

 Copyright © Huawei Technologies Co., Ltd.

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 255.

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.

If a user that belongs to this domain is online, you cannot run the **undo domain** command to delete the domain.

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.

 Copyright © Huawei Technologies Co., Ltd.

The device supports a maximum of 256 domains, including the **default** and **default_admin** domains.

Example

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

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

Related Topics

19.1.41 display domain

19.1.51 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.
admin	Configures a domain for administrators. If this parameter is not specified, the domain for common access users is configured.	-

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.50 domain (AAA view)

19.1.41 display domain

19.1.52 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.

Format

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

undo domain-location

 Copyright © Huawei Technologies Co., Ltd.

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 interface view, the configuration takes effect for only the users connected to this interface. 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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.1.33 display aaa configuration

19.1.53 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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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.

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 /
```

Related Topics

19.1.33 display aaa configuration

19.1.60 local-user

19.1.54 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.

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.	-

 Copyright © Huawei Technologies Co., Ltd.

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 interface view, the configuration takes effect for only the users connected to this interface. 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.

 Copyright © Huawei Technologies Co., Ltd.

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

Related Topics

19.1.33 display aaa configuration

19.1.55 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.	-

Views

Service scheme view

 Copyright © Huawei Technologies Co., Ltd.

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 for administrators. For common users, the function takes effect only for PPPoE and Portal 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.
- The idle-cut function takes effect only after the idle time and traffic threshold are configured. To configure the traffic threshold, run the **idle-cut** *idle-time flow-value* command. To configure the idle time, use the value of *idle-time* configured on the device or the value (carried in RADIUS attribute 28 Idle-Timeout) authorized by the RADIUS server. If both values exist, the value authorized by the RADIUS server has a higher priority.

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 huawei
[Huawei-aaa-service-huawei] idle-cut 1 10
```

Related Topics

19.1.47 display service-scheme

19.1.56 ip-pool (service scheme view)

Function

The **ip-pool** command sets the IP address pool bound to a service scheme or moves the location of a configured IP address pool bound to a service scheme.

The **undo ip-pool** command deletes the IP address pool bound to a service scheme. If no parameter is specified, all the IP address pools bound to a service scheme are deleted.

By default, no IP address pool is bounded in a service scheme.

 Copyright © Huawei Technologies Co., Ltd.

Format

ip-pool *pool-name* [**move-to** *new-position*]

undo ip-pool [*pool-name*]

Parameters

Parameter	Description	Value
pool-name	Specifies the IP address pool name.	The name is a string of 1 to 64 characters and can contain letters, digits (0-9), dots (.), hyphens (-), and underscores (_).
move-to *new-position*	Moves the location of a configured IP address pool bound to a service scheme.	The value range varies according to the number of configured address pools bound to a domain. For example, if there are ten IP address pools in a domain, the value ranges from 1 to 10. The number of IP address pools ranges from 1 to 16.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command limits the range of IP addresses of users in a service scheme. The **ip-pool** command is used to reference the configured address pool to a service scheme. An IP address pool is configured using the **ip pool (system view)** command.

Prerequisites

A global IP address pool has been created using the **8.3.83 ip pool (system view)** command and the address range has been specified using the **8.3.92 network (IP address pool view)** command.

Copyright © Huawei Technologies Co., Ltd.

Example

Set the IP address pool **pool1** for the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] ip pool pool1
[Huawei-ip-pool-pool1] network 192.168.100.0 mask 24
[Huawei-ip-pool-pool1] quit
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] ip-pool pool1
```

Change the position of the IP address **ippool1** in the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] ip pool ippool1
[Huawei-ip-pool-ippool1] network 192.168.100.0 mask 24
[Huawei-ip-pool-ippool1] quit
[Huawei] ip pool ippool2
[Huawei-ip-pool-ippool2] network 192.168.200.0 mask 24
[Huawei-ip-pool-ippool2] quit
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] ip-pool ippool1
[Huawei-aaa-service-svcscheme1] ip-pool ippool2
[Huawei-aaa-service-svcscheme1] ip-pool ippool1 move-to 2
```

Related Topics

19.1.47 display service-scheme

8.3.83 ip pool (system view)

19.1.57 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

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.1.58 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 enabled.

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]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.1.73 password history record number

19.1.59 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 the 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

 Copyright © Huawei Technologies Co., Ltd.

After the **undo local-aaa-user password policy administrator** command is executed, the administrator password policy will be disabled, causing a security risk.

Example

Enable the local administrator password policy 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]
```

Related Topics

19.1.60 local-user

19.1.72 password expire

19.1.70 password alert before-expire

19.1.71 password alert original

19.1.73 password history record number

19.1.60 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, the local user **admin** exists in the system. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it. The irreversible encryption algorithm is used, the level is 15, and service type is http.

Format

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

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

 Copyright © Huawei Technologies Co., Ltd.

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 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
access-limit *max-number*	Specifies the maximum number of connections established by a specified user. 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 type on different models.
ftp-directory *directory*	Specifies the directory that an FTP user can 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 has been set using the **3.11.59 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
opt	Indicates that the challenge in the MD5 algorithm takes precedence. By default, the password takes precedence.	-
idle-cut	Indicates the idle-cut function for local user. 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. After the **local-user idle-cut** command is run, the device periodically detects the specified users. If the traffic volume of a user within the idle-cut period is lower than the threshold, the user is disconnected. By default, the idle-cut period is 10 minutes and threshold is 600K bytes. If the service scheme bound to an AAA domain contains the idle-cut parameters configured by the **19.1.55 idle-cut (service scheme view)** command, these idle-cut parameters take effect.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
idle-timeout *minutes* [*seconds*]	Specifies the idle timeout interval. • *minutes* indicates the idle timeout interval, in minutes. • *seconds* indicates the idle timeout interval, in seconds. If this parameter is not specified, the device uses the idle timeout interval configured by the **3.8.15 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.	The value of *minutes* is an integer that ranges from 0 to 35791, in minutes. The value of *seconds* is an integer that ranges from 0 to 59, in seconds.
privilege level *level*	Specifies the level of a local user. After logging in to the device, a user can run only the commands of the same level or lower levels. **NOTE** If this parameter is not specified, the user level is 0.	The value is an integer that ranges from 0 to 15. A larger value indicates a higher level of a user.

Copyright © Huawei Technologies Co., Ltd.

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, so security is low. • 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 special encryption algorithm. User security is ensured. If this parameter is not specified, the device automatically allocates the default password to the user. For security purposes, change the password immediately and update the password periodically. 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.	The value is a case-sensitive string without question marks (?) or spaces. • If the **cipher** parameter is specified, the value of *password* can be a plain text of 8 to 128 characters or a cipher-text password of 48 to 188 characters. • If the **irreversible-cipher** parameter is specified, the value of *password* can be a plain text of 8 to 128 characters or a cipher-text password of 68 characters. A simple local user password may bring security risks. The user password must consist of two types of characters, including uppercase letters, lowercase letters, numerals, and special characters. In addition, the password cannot be the same as the user name or user name in an inverse order.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	NOTICE It is recommended that you set the user password when creating a user. The interaction method using the **19.1.66 local-user password** command is recommended.	
state { **active** | **block** }	Indicates the state of a local user. • **active**: indicates the active state. The device accepts and processes the authentication request from the user, and allows the user to change the password. • **block**: indicates the 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.	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 --.

 Copyright © Huawei Technologies Co., Ltd.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To facilitate device maintenance, run the **local-user** command on the device to create a local user and set parameters such as the password, user level, and FTP directory.

Prerequisites

Before adding a local user to a user group, ensure that the user group has been created using the **19.6.150 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 level. The attributes include password, user level, maximum number of access users, and account validity period.

  After you change the rights (for example, the password, level, FTP directory, idle timeout interval, or status) of a local account, the rights of users already online do not change. The change takes effect when the user next goes online.
- The user name function may be invalid due to improper configuration of the domain name delimiter.
- A maximum of 512 local accounts can be configured.
- V200R005C00 and later versions use new encryption mechanism. After the AR is upgraded to V200R005C00 and later versions, you are advised to change the password to a more secure password.

  V200R005C00 and later versions use new encryption mechanism. If the version is rolled back, the original version cannot identify the password configured in V200R005C00 and later versions. As a result, the configuration becomes invalid. To ensure that the password takes effect after rollback, during rollback, restore the password-relevant configuration in the configuration file to the configuration before the upgrade or change the password-relevant configuration in the configuration file to the configuration that can be identified by the original version.

 Copyright © Huawei Technologies Co., Ltd.

- 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.
- The **idle-cut** command configured in the service scheme view takes effect for administrators. For common users, the function takes effect only for PPPoE and Portal users.

Example

Create a local user **user1**, and set the domain name to **vipdomain**, the password to **admin@12345** in cipher text, 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 admin@12345 access-limit 100 idle-timeout 10
```

Related Topics

19.1.42 display local-user

19.1.61 local-user account-type

Function

The **local-user account-type** command sets the account type for a local user.

The **undo local-user account-type** command restores the default account type for a local user.

By default, the account type of local users is not specified.

Format

local-user *user-name* **account-type cmcc-tr069**

undo local-user *user-name* **account-type**

Parameters

Parameter	Description	Value
user-name	Specifies the local user of which the account type needs to be set.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cmcc-tr069	Sets the account type of the local user to CMCC-TR069.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

TR-069, also called CPE WAN Management Protocol (CWMP), defines the communication mechanism between the Customer Premises Equipment (CPE) and Auto-Configuration Server (ACS) and allows the ACS to centrally manage CPEs.

This command is applicable to the following scenarios:

- After a user is created by the **local-user** command, set the account type of the user to CMCC-TR069, which indicates a TR069 administrator of China Mobile.
- When a device functions as a CPE, if the ACS of China Mobile creates an administrator on the CPE through TR-069, the CPE automatically executes this command to set the account type of the administrator to CMCC-TR069.

After the CMCC-TR069 administrator is created, the administrator can manage the device through ACS. When the device restores configurations after a reboot, the ACS quickly obtains information about the CMCC-TR069 administrator.

Precautions

If the TR-069 function is not enabled by the **4.2.16 set operator-code cmcc** command, this command cannot be executed.

Only one CMCC-TR069 user is supported on a device.

Example

Set the account type of the local user user1@vipdomain to CMCC-TR069.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user user1@vipdomain account-type cmcc-tr069
```

Related Topics

19.1.60 local-user

19.1.42 display local-user

 Copyright © Huawei Technologies Co., Ltd.

19.1.62 local-user bind-ip

Function

The **local-user bind-ip** command allocates a fixed IP address to a local user.

The **undo local-user bind-ip** command restores the default setting.

By default, no fixed IP address is allocated to the local user.

Format

local-user *user-name* **bind-ip** *ip-address*

undo local-user *user-name* **bind-ip**

Parameters

Parameter	Description	Value
user-name	Specifies the name of a local user.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
ip-address	A fixed IP address is allocated to the local user.	The value is in dotted decimal notation.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a local user passes authentication, run the **local-user bind-ip** command to allocate a fixed IP address to the user. Then the user has the network access right corresponding to the allocated IP address. For example, if a public network address is allocated, the user can access the public network; if a private network address is allocated, the user can access the private network. When the user goes offline and online again, the IP address is still bound to the user.

Precautions

After you run this command to allocate a fixed IP address to a local user, you need to exclude this IP address from the DHCP address pool, preventing this IP address from being allocated to another user to cause an IP address conflict.

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind IP address 192.168.1.1 to the local user **hello@163.net**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user hello@163.net bind-ip 192.168.1.1
```

19.1.63 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.
- After the user that passes local authentication changes the password, the user must type the new password to pass local authentication.
- 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 password of a local user may bring security risks. When a local user changes the password, the new password must be a string of 8 to 128 characters and must contain at least two types of the following: uppercase

 Copyright © Huawei Technologies Co., Ltd.

letters, lowercase letters, digits, and special characters. In addition, the new password cannot be the same as the user name or the user name in a reverse order.

- For device security purposes, change the password periodically.

Example

The local user changes 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, numer
als and special characters.
Please enter old password:
Please enter new password:
Please confirm new password:
Info: The password is changed successfully.
```

19.1.64 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 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.60 local-user

19.1.65 local-user idle-cut

Function

The **local-user idle-cut** command enables the idle-cut function for local users.

The **undo local-user idle-cut** command restores the default setting.

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

Format

local-user *user-name* **idle-cut**

undo local-user *user-name* **idle-cut**

Parameters

Parameter	Description	Value
user-name	Specifies a user name.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

 Copyright © Huawei Technologies Co., Ltd.

Views

AAA 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. After this command is executed, the device periodically detects the specified users. If the traffic volume of a user within the idle-cut period is lower than the threshold, the user is disconnected. By default, the idle-cut period is 10 minutes and threshold is 600K bytes. If the service scheme bound to an AAA domain contains the idle-cut parameters configured by the **19.1.55 idle-cut (service scheme view)** command, these idle-cut parameters take effect.

Precautions

When local authentication is used, this command is valid to only common users (for example, NAC and PPP users). To configure idle-cut for administrators, run the **local-user idle-timeout** command.

Example

Enable the idle-cut function for local user **hello@163.net**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user hello@163.net idle-cut
```

19.1.66 local-user password

Function

The **local-user password** command configures a password for a local account.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

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 8~128 case-sensitive characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
user-name	Specifies the local user name.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

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, numerals, and special characters. In addition, the password cannot be the same as the user name or user name in a reverse order.

V200R005C00 and later versions use new encryption mechanism. After the AR is upgraded to V200R005C00 and later versions, you are advised to change the password to a more secure password.

V200R005C00 and later versions use new encryption mechanism. If the version is rolled back, the original version cannot identify the password configured in V200R005C00 and later versions. As a result, the configuration becomes invalid. To ensure that the password takes effect after rollback, during rollback, restore the password-relevant configuration in the configuration file to the configuration before the upgrade or change the password-relevant configuration in the configuration file to the configuration that can be identified by the original version.

Example

Set the password to abc@#123456 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 abc@#123456
```

 Copyright © Huawei Technologies Co., Ltd.

```
Please confirm password:          //Confirm the password abc@#123456
Info: Add a new user.
```

Related Topics

19.1.42 display local-user

19.1.67 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** | **bind** | **ftp** | **http** | **ppp** | **ssh** | **sslvpn** | **telnet** | **terminal** | **web** | **x25-pad** } *

undo local-user *user-name* **service-type**

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 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
8021x	Indicates an 802.1X user.	-
bind	Indicates an IP session user.	-
ftp	Indicates an FTP user.	-
http	Indicates an HTTP user, which is usually used for web system login.	-
ppp	Indicates a PPP user.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ssh	Indicates an SSH user.	-
sslvpn	Indicates an SSLVPN 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.	-

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: FTP, HTTP, SSH, Telnet, x25-pad, and Terminal
- Common: 802.1X, bind, ppp, sslvpn, 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

 Copyright © Huawei Technologies Co., Ltd.

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.

  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
```

Related Topics

19.1.60 local-user

19.1.42 display local-user

19.1.68 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 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 **19.7.24 time-range** command.

Precautions

If you run the **local-user time-range** and **19.1.64 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 huawei 9:00 to 18:00 working-day
[Huawei] aaa
[Huawei-aaa] local-user hello@163.net time-range huawei
```

Related Topics

19.1.42 display local-user

 Copyright © Huawei Technologies Co., Ltd.

19.1.69 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<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
```

Related Topics

19.1.45 display recording-scheme

19.1.77 recording-scheme

19.1.70 password alert before-expire

Function

The **password alert before-expire** command to set the password expiration prompt days.

The **undo password alert before-expire** command restores the default password expiration prompt days.

By default, the number of password expiration prompt days is 30 days.

Format

password alert before-expire *day*

undo password alert before-expire

Parameters

Parameter	Description	Value
day	Indicates how long the system displays a prompt before the password expires. If the value is set to 0, the device does not prompt users that the passwords will expire.	The value is an integer that ranges from 0 to 999, in days. The default value is 30.

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 more days the password is valid for. If the number of days is less than the prompt days set in this

 Copyright © Huawei Technologies Co., Ltd.

command, the device notifies the user in how many days the password will expire and asks the user whether they want to change the password.

- If the user changes the password, the device records the new password and modification time.
- If the user does not change the password or fails to change the password, the user can still log in as long as the password has not expired.

Example

Set the number of password expiration prompt days to 90.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-aaa-user password policy administrator
[Huawei-aaa-lupp-admin] password alert before-expire 90
```

19.1.71 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**:

 Copyright © Huawei Technologies Co., Ltd.

  - 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, and the initial password is the default password, the device does not allow the user to log in. If the initial password is not the default password, the device allows 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. The device displays a prompt message in this situation).

Precautions

This function is only valid for Telnet 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
```

19.1.72 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.

Format

password expire *day*

undo password expire

Parameters

Parameter	Description	Value
day	Indicates 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.

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 local user's 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 selects **Y**, 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 user cannot log in.

Precautions

Changing the system time will affect the password validity status.

After this command is executed, the device checks whether the password expires every minute; therefore, there may be a time difference within 1 minute.

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
```

 Copyright © Huawei Technologies Co., Ltd.

19.1.73 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, five historical passwords are recorded for each user.

Format

password history record number *number*

undo password history record number

Parameters

Parameter	Description	Value
number	Indicates 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.

 Copyright © Huawei Technologies Co., Ltd.

After the historical password recording function is disabled, the device does not record historical passwords; however, the passwords that have been stored are not deleted.

Example

Set the maximum number of historical passwords recorded for each 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
```

19.1.74 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.

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.
all	Deletes the permitted domain for all WLAN users.	-

Views

Authentication profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a permitted domain is specified on an authentication profile or an interface, 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.

If the service set mapping the interface has been bound to the radio, you cannot run this command. The command can be configured only after the service set is unbound from the radio.

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
```

Related Topics

19.1.50 domain (AAA view)

19.1.75 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.

Format

qos-profile *profile-name*

undo qos-profile *profile-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the QoS profile bound to the service scheme.	The value is 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 **19.1.90 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.

Prerequisites

A QoS profile has been created using the **20.3.18 qos-profile** command.

Precautions

The RADIUS server can also deliver a QoS profile and the CAR to the device. (The CAR can also be set in a QoS profile.)

When the server delivers the CAR and a QoS profile using Huawei extended RADIUS attributes:

- If the server delivers the CAR, the device uses the CAR.
- If the server delivers a QoS profile, the device uses the QoS profile.
- If the server delivers the CAR and a QoS profile, the device preferentially uses the CAR.
- If the server does not deliver the CAR and QoS profile, the device uses the QoS profile bound to the service scheme.

Example

Bind the QoS profile **abc** to the service scheme **huawei**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme huawei
[Huawei-aaa-service-huawei] qos-profile abc
```

Related Topics

19.1.90 service-scheme (AAA view)

 Copyright © Huawei Technologies Co., Ltd.

19.1.76 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 **19.3.14 hwtacacs-server template** command.

Example

Associate the recording scheme **scheme0** with the HWTACACS server template **tacacs1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<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
```

Related Topics

19.3.2 display hwtacacs-server template

19.1.45 display recording-scheme

19.3.14 hwtacacs-server template

19.1.77 recording-scheme

19.1.77 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

Copyright © Huawei Technologies Co., Ltd.

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]
```

Related Topics

19.1.29 cmd recording-scheme

19.1.45 display recording-scheme

19.1.69 outbound recording-scheme

19.1.76 recording-mode hwtacacs

19.1.93 system recording-scheme

Copyright © Huawei Technologies Co., Ltd.

19.1.78 remote-aaa-user authen-fail

Function

The **remote-aaa-user authen-fail** command enables the remote AAA authentication account locking function, and sets the authentication retry interval, maximum number of consecutive authentication failures, and account locking period.

The **undo remote-aaa-user authen-fail** command disables the remote AAA authentication account locking function.

By default, the remote AAA account locking function is enabled, authentication retry interval is 30 minutes, maximum number of consecutive authentication failures is 30, and account locking period is 30 minutes.

Format

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

undo remote-aaa-user authen-fail

Parameters

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

To ensure account security, you can enable the device to lock the accounts that fail in remote AAA authentication. If a user enters incorrect account and password

 Copyright © Huawei Technologies Co., Ltd.

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 is valid only for remote AAA authentication and is invalid for local authentication.
- In scenarios where an active/standby switchover is performed, the originally locked account is automatically unlocked.
- After the remote AAA authentication account locking function is disabled using the **undo remote-aaa-user authen-fail** command, the originally locked account is automatically unlocked.

Example

Enable the remote AAA account locking function, 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] remote-aaa-user authen-fail retry-interval 5 retry-time 3 block-time 5
```

Disable the remote AAA account locking function.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] undo remote-aaa-user authen-fail
Info: All blocked users will unblock. Continue?[Y/N] y
```

Related Topics

19.1.46 display remote-user authen-fail

19.1.79 remote-user authen-fail unblock

19.1.79 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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
```

Related Topics

19.1.46 display remote-user authen-fail

19.1.80 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** }

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.1.81 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
```

19.1.82 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
```

 Copyright © Huawei Technologies Co., Ltd.

19.1.83 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
```

19.1.84 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**

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.1.73 password history record number

19.1.85 route set acl

Function

The **route set acl** command configures the local subnet information to be sent to the remote end.

The **undo route set acl** command restores the default setting.

By default, no local subnet information is sent to the remote end.

 Copyright © Huawei Technologies Co., Ltd.

Format

route set acl *acl-number*

undo route set acl

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL to be sent to the remote end.	The value is an integer that ranges from 3000 to 3999.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The headquarters and a branch use virtual tunnel interfaces to set up an IPSec tunnel. When you apply an IPSec profile to the Tunnel-template interface on the headquarters gateway and apply an IPSec profile to the tunnel interface on the branch gateway, you can run this command to send the source IP address configured in an ACL to the remote end. The source IP address can be used to generate subnet route information.

Precautions

This command can send subnet route information only when it is used together with the **19.1.86 route set interface** command.

Before running this command, you are advised to run the **19.7.4 acl (system view)** command to create an ACL.

Example

Send information about ACL 3000 to the remote end.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
[Huawei-acl-adv-3000] quit
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] route set acl 3000
```

Related Topics

19.7.4 acl (system view)

 Copyright © Huawei Technologies Co., Ltd.

19.1.47 display service-scheme

19.1.86 route set interface

Function

The **route set interface** command configures the address of the interface bound to the IPSec tunnel to be sent to the remote end.

The **undo route set interface** command restores the default setting.

By default, no address of the interface bound to the IPSec tunnel is sent to the remote end.

Format

route set interface

undo route set interface

Parameters

None

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The headquarters and a branch use virtual tunnel interfaces to set up an IPSec tunnel. You can run this command to send the address of the interface bound to the IPSec tunnel to the remote end. This address can be used to generate subnet route information.

Precautions

If you do not configure this command, packets cannot be sent through the IPSec tunnel even if the IPSec tunnel is successfully established and route information is sent to the remote end.

Example

Configure the address of the interface bound to the IPSec tunnel to be sent to the remote end.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] route set interface
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.1.47 display service-scheme

19.1.87 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.

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 **19.1.88 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
```

 Copyright © Huawei Technologies Co., Ltd.

19.1.88 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 the 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 the EAP authentication is configured for 802.1X users, the device removes the security string and encapsulates it into the HW-SecurityStr attribute.

Format

security-name-delimiter *delimiter*

undo security-name-delimiter

Parameters

Parameter	Description	Value
delimiter	Specifies a delimiter for a security string.	The value is \ / : < > | @ ' % 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 the ***securitystring** and only uses **username@domain** for authentication.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

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

19.1.89 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

 Copyright © Huawei Technologies Co., Ltd.

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 **huawei**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme srvscheme1
[Huawei-aaa-service-srvscheme1] quit
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] service-scheme srvscheme1
```

Related Topics

19.1.47 display service-scheme

19.1.90 service-scheme (AAA view)

19.1.90 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*

 Copyright © Huawei Technologies Co., Ltd.

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

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.

A maximum of 256 service schemes can be configured on the device.

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]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.1.47 display service-scheme
19.1.89 service-scheme (aaa domain view)

19.1.91 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.	-
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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.7.24 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
```

Related Topics

19.1.50 domain (AAA view)

19.1.92 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.

Format

statistic enable

undo statistic enable

 Copyright © Huawei Technologies Co., Ltd.

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 **19.1.37 display access-user (All views)** command to view traffic statistics of users.

Precautions

The **20.6.2 statistics enable (QoS profile view)** command executed in the QoS profile view collects DAA service statistics for domain users. The statistics include the number of bytes matching each tariff level. This command collects non-DAA service statistics. The device sends the two types of statistics to the accounting server for flexible accounting.

Only Portal authentication users on the WAN-side interface and PPP authentication users support this command.

Example

Enable traffic statistics collection for domain users.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] statistic enable
```

Related Topics

19.1.41 display domain

19.1.93 system recording-scheme

Function

The **system recording-scheme** command applies a policy in a recording scheme to record the system events.

 Copyright © Huawei Technologies Co., Ltd.

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 helps 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-aaa-recording-scheme] quit
[Huawei-aaa] system recording-scheme scheme
```

Related Topics

19.1.45 display recording-scheme

19.1.77 recording-scheme

19.1.94 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.

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.

 Copyright © Huawei Technologies Co., Ltd.

- 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.

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
```

Related Topics

19.6.150 user-group

19.1.95 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, a device checks password complexity.

Format

user-password complexity-check

undo user-password complexity-check

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can choose whether to enable password complexity check.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

To ensure device security, do not disable password complexity check, and change the password periodically.

Example

Disable password complexity check.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] undo user-password complexity-check
```

Related Topics

19.1.60 local-user

19.1.96 wins (service scheme view)

Function

The **wins** command configures the primary or secondary WINS server address in the service scheme view.

The **undo wins** command deletes a primary or secondary WINS server address.

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

Format

wins *ip-address* [**secondary**]

undo wins [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Indicates the WINS server address configured in a service scheme.	The value is in dotted decimal notation.
secondary	Indicates that the IP address of the secondary WINS server is configured.	-

Views

service scheme view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The AAA service scheme allows the WINS server address to be bound. IPSec binds the AAA service scheme to the IPSec policy template and sends the WINS server address to users.

Example

Configure the WINS server address in the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] wins 10.1.1.1
```

Related Topics

19.1.47 display service-scheme

19.1.97 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.2 RADIUS Configuration Commands

19.2.1 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** } [**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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hyphen-split	Indicates that the hyphen (-) 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 called-station-id attribute uses the XXXX-XXXX-XXXX or XXXX.XXXX.XXXX format.	-
mode2	Indicates that the MAC address in the called-station-id attribute uses the 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 huawei
[Huawei-radius-huawei] called-station-id mac-format dot-split mode2 uppercase
```

Related Topics

19.2.9 display radius-server configuration

19.2.2 calling-station-id mac-format

 Copyright © Huawei Technologies Co., Ltd.

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**separator**xxxx**separator**xxxx" format.	-
mode2	Indicates that the MAC address in the calling-station-id attribute uses the "xx**separator**xx**separator**xx**separator**xx**separator**xx**separator**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

 Copyright © Huawei Technologies Co., Ltd.

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 huawei
[Huawei-radius-huawei] calling-station-id mac-format dot-split mode2 uppercase
```

Related Topics

19.2.9 display radius-server configuration

19.2.3 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 **19.2.15 radius-attribute disable** command on the device to disable RADIUS attributes that are not supported by the RADIUS server or run the **19.2.20 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 19-20 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.
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 19-21 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.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.2.15 radius-attribute disable

19.2.20 radius-attribute translate

19.2.4 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
-------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-22 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.

Related Topics

19.2.14 radius-attribute check

19.2.5 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

 Copyright © Huawei Technologies Co., Ltd.

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 19-23 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.

Related Topics

19.2.15 radius-attribute disable

 Copyright © Huawei Technologies Co., Ltd.

19.2.6 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 19-24 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.

Related Topics

19.2.20 radius-attribute translate

19.2.7 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.

 Copyright © Huawei Technologies Co., Ltd.

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.
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
```

Table 19-25 Description of the display radius-server accounting-stop-packet command output

Item	Description
Time Stamp	Timestamp of an accounting-stop packet.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Resend Times	Number of times that accounting-stop packets have been retransmitted.
Session Time	Session time, in seconds.
Username	User name.

Related Topics

19.2.23 radius-server accounting-stop-packet resend
19.2.48 reset radius-server accounting-stop-packet

19.2.8 display radius-server authorization configuration

Function

The **display radius-server authorization configuration** command displays the configuration of RADIUS authorization servers.

Format

display radius-server authorization configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **radius-server authorization** command to configure an authorization server, run the **display radius-server authorization configuration** command to check whether the authorization server configuration 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
IP-Address      Shared-key              Group                   Protect      Ack-reserved-interval
--------------------------------------------------------------------------------
10.10.1.114     ****************        -                       Y                 20
vpn-instance : -
--------------------------------------------------------------------------------
1 RADIUS authorization server(s) in total
```

Table 19-26 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 configurations in the RADIUS server template. To configure this field, run the **19.2.29 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 configurations in the RADIUS server template. To configure this field, run the **19.2.30 radius-server authorization attribute-encode-sameastemplate** command.
User information match type	Method used by a device to perform a match check between the RADIUS attribute in the received CoA or DM Request packet and user information on the device. The values are as follows: • all: The device performs a match check between all attributes in the received CoA or DM Request packet and user information on the device. • any: The device performs a match check between an attribute in the received CoA or DM Request packet and user information on the device. To configure this field, run the **19.2.32 radius-server authorization match-type** command.
IP-Address	IP address of a RADIUS authorization server. To configure this field, run the **radius-server authorization** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Shared-key	Shared key of the RADIUS authorization server. To configure this field, run the **radius-server authorization** command.
Group	RADIUS server group matching the RADIUS authorization server. To configure this field, run the **radius-server authorization** command.
Ack-reserved-interval	Holdtime of RADIUS authorization response packets. To configure this field, run the **radius-server authorization** command.
Protect	Whether the security hardening function is enabled. To configure this field, run the **radius-server authorization** command.
vpn-instance	Name of the VPN instance that the RADIUS authorization server is bound to. To configure this field, run the **radius-server authorization** command.

Related Topics

19.2.28 radius-server authorization

19.2.9 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*]

 Copyright © Huawei Technologies Co., Ltd.

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
  Protocol-version              : standard
  Traffic-unit                  : B
  Shared-secret-key             : %^%#O09i(W[^YT4g#Z37Nct9$IK#TH(-B6-1|<;q|D)"%^%#
  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                  : -
  NAS-IPv6-Address              : ::
  Server algorithm              : master-backup
  Detect-interval(in second)    : 60
  Testuser-username             : huawei
  Testuser-ciperpwd             : %^%#.5*EDl^j_WXg[#Z>plj8;k|8.s*ju<_F~g9k`0*9%^%#
  Authentication Server 1       : 10.7.66.66     Port:1812  Weight:80  [UP]
                                  Vrf:- LoopBack:NULL Vlanif:NULL
                                  Source IP: ::
  Authentication Server 2       : 10.7.66.67     Port:1812  Weight:80  [UP]
                                  Vrf:- LoopBack:NULL Vlanif:NULL
```

 Copyright © Huawei Technologies Co., Ltd.

```
                          Source IP: ::
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 19-27 Description of the **display radius-server configuration template** *template-name* command output

Item	Description
Server-template-name	Name of a RADIUS server template. To configure this item, run the **radius-server template** command.
Protocol-version	RADIUS protocol version: • standard • huawei • iphotel • portal
Traffic-unit	Traffic unit in the RADIUS server template: • B: Byte • KB: Kilobyte • MB: Megabyte • GB: Gigabyte To configure this item, run the **radius-server traffic-unit** command.
Shared-secret-key	Shared key in the RADIUS server template. To configure this item, 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 configure this item, run the **19.2.40 radius-server retransmit timeout dead-time** command.
Retransmission	Number of times RADIUS packets are retransmitted. To configure this item, run the **19.2.40 radius-server retransmit timeout dead-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
EndPacketSendTime	Number of times RADIUS accounting-stop packets are retransmitted. To configure this item, run the **radius-server accounting-stop-packet resend** command.
Dead time(in minute)	Interval for the primary RADIUS server to revert to the active status. To configure this item, run the **19.2.40 radius-server retransmit timeout dead-time** 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 configure this item, run the **19.2.47 radius-server user-name domain-included** command.
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 configure this item, run the **19.2.1 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. • Old: Uses the old format of the NAS-Port-ID attribute. To configure this item, run the **19.2.39 radius-server nas-port-id-format** command.
Service-type	Service type.
NAS-IPv6-Address	NAS IPv6 address in RADIUS packets.

Copyright © Huawei Technologies Co., Ltd.

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 configure this item, run the **19.2.24 radius-server algorithm** command.
Detect-interval(in second)	Automatic detection interval for RADIUS servers. To configure this item, run the **radius-server detect-server** command.
Testuser-username	User name for automatic RADIUS server detection. To configure this item, run the **radius-server testuser** command.
Testuser-ciperpwd	User password for automatic RADIUS server detection. To configure this item, 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 configure this item, 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 configure this item, run the **radius-server authentication** command.
Accounting Server 1	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the primary RADIUS accounting server. To configure this item, run the **radius-server accounting** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Accounting Server 2	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the secondary RADIUS accounting server. To configure this item, run the **radius-server accounting** command.

19.2.10 display radius-server dead-interval dead-count

Function

The **display radius-server dead-interval dead-count** command displays configuration information about the RADIUS server detection interval and maximum number of consecutive unacknowledged packets in each detection interval.

Format

display radius-server { **dead-interval** | **dead-count** }

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the RADIUS server detection interval and maximum number of consecutive unacknowledged packets in each detection interval are configured using the **19.2.33 radius-server dead-interval dead-count** command, you can run the **display radius-server** { **dead-interval** | **dead-count** } command to check configuration information about the RADIUS server detection interval 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.
```

 Copyright © Huawei Technologies Co., Ltd.

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.
```

Table 19-28 Description of the **display radius-server** { **dead-interval** | **dead-count** } 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.

19.2.11 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<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 19-29 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.
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.

19.2.12 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* }

 Copyright © Huawei Technologies Co., Ltd.

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
```

 Copyright © Huawei Technologies Co., Ltd.

```
Tail       = 1311
ProbeID    = 255
------------------------------------------------------------------------------
```

Table 19-30 Description of the **display radius-server item** template command output

Item	Description
STState	Status of the RADIUS server template. ● 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 that the RADIUS server is in UP status. ● state-down: indicates that the RADIUS server is in DOWN status. ● state-probe: indicates that the RADIUS server is in detection status.
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.

 Copyright © Huawei Technologies Co., Ltd.

19.2.13 display snmp-agent trap feature-name radius all

Function

The **display snmp-agent trap feature-name radius all** command displays the status of all traps on the RDS module.

Format

display snmp-agent trap feature-name radius all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the RDS module, you can run this command to check the status of all traps on the RDS module. To enable the trap function for the RDS module, run the **snmp-agent trap enable feature-name radius** command.

Prerequisites

The SNMP function has been enabled on the device.

Example

Display the status of all traps on the RDS module.

```
<Huawei>display snmp-agent trap feature-name radius all
------------------------------------------------------------------------------
Feature name: radius
Trap number : 4
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwRadiusAuthServerUp          off                     off
hwRadiusAuthServerDown        off                     off
hwRadiusAcctServerUp          off                     off
hwRadiusAcctServerDown        off                     off
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-31 Description of the **display snmp-agent trap feature-name radius all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.
Trap name	Name of a trap. Traps on the RDS module include: • hwRadiusAuthServerUp: The device sends a Huawei proprietary trap when it detects that communication with the RADIUS authentication server is restored. • hwRadiusAuthServerDown: The device sends a Huawei proprietary trap when it detects that communication with the RADIUS authentication server is interrupted. • hwRadiusAcctServerUp: The device sends a Huawei proprietary trap when it detects that communication with the RADIUS accounting server is restored. • hwRadiusAcctServerDown: The device sends a Huawei proprietary trap when it detects that communication with the RADIUS accounting server is interrupted.
Default switch status	Default status of the trap function: • on: The trap function is enabled by default. • off: The trap function is disabled by default.
Current switch status	Trap status: • on: The trap is enabled. • off: The trap is disabled.

Related Topics

19.2.49 snmp-agent trap enable feature-name radius

19.2.14 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.2.3 display radius-attribute

19.2.15 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

Copyright © Huawei Technologies Co., Ltd.

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 **19.2.26 radius-server attribute translate** command.

Precautions

Before disabling RADIUS attributes, run the **19.2.3 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
```

Related Topics

19.2.3 display radius-attribute

19.2.44 radius-server template

19.2.16 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**]

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.2.9 display radius-server configuration

19.2.17 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.2.9 display radius-server configuration

19.2.18 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 mac** | **user-type ipsession**]

undo radius-attribute set *attribute-name*

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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
attribute-value	Indicates the value of the attribute to be modified.	The value of *attribute-value* is automatically displayed.
auth-type mac	Sets the user authentication mode to MAC address 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.

 Copyright © Huawei Technologies Co., Ltd.

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, NAS-IP-Address, NAS-IPv6-Address, CHAP-Password, CHAP-Challenge, EAP-Message, Framed-Interface-Id, Framed-IPv6-Prefix, and Message-Authenticator.

- The type of the attribute modified by the **radius-attribute set** command cannot be changed.
- The **radius-attribute set service-type** *attribute-value* { **auth-type mac** | **user-type ipsession** } command has a higher priority than the **radius-attribute set service-type** *attribute-value* command.
- A maximum of 8 attributes can be set in a RADIUS server template.
- If the value of the HW-Output-Committed-Information-Rate attribute is changed to 0, sent packets do not carry this attribute.

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
```

Related Topics

19.2.44 radius-server template

19.2.19 radius-attribute service-type with-authenonly-reauthen

Function

The **radius-attribute service-type with-authenonly-reauthen** command set 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, this command is not configured and 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

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A large number of users are online at the same time and each user has a lot of authorization information. If the users need to be reauthenticated, the device delivers authorization information to each user after the authentication is successful. It is difficult for the device to process a lot of authorization information. As a result, users go offline due to authorization failures. 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 this 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 after the Service-Type attribute on the RADIUS server is set to Authenticate Only.

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
```

Related Topics

19.2.9 display radius-server configuration

19.2.20 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** } *

 Copyright © Huawei Technologies Co., Ltd.

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.	-
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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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

 Copyright © Huawei Technologies Co., Ltd.

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 user hopes that the device can 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.
- 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.2.3 display radius-attribute
19.2.6 display radius-attribute translate
19.2.26 radius-server attribute translate
19.2.44 radius-server template

19.2.21 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.2.44 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
```

Related Topics

19.2.9 display radius-server configuration

19.2.44 radius-server template

19.2.22 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.

Copyright © Huawei Technologies Co., Ltd.

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*] *

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**]]]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.
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.
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 vpn-instance must already exist.
source loopback *interface-number*	Specifies the number of a loopback interface.	The loopback interface must already exist.
source ip-address *ipv4-address*	Specifies the source IPv4 address of a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.
source ip-address *ipv6-address*	Specifies the source IPv6 address of a RADIUS accounting server. This address cannot be a VRRP6 virtual address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	The value is an integer that ranges from 0 to 100.

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.

Example

Configure the primary RADIUS accounting server.

 Copyright © Huawei Technologies Co., Ltd.

```
<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
```

Related Topics

19.2.9 display radius-server configuration

19.2.23 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.2.9 display radius-server configuration

19.2.24 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 primary/secondary.

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.	-

 Copyright © Huawei Technologies Co., Ltd.

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.	-
master-backup	Sets the algorithm for selecting RADIUS servers to primary/secondary.	-

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%

If the algorithm for selecting RADIUS servers is set to the single user-based algorithm, authentication server information is saved in the authentication phase, and the device preferentially sends an accounting request to the accounting server in the accounting phase when the accounting server is the same as the authentication server. If the algorithm for selecting RADIUS servers is set to the packet-based algorithm, authentication server information is not saved in the

 Copyright © Huawei Technologies Co., Ltd.

authentication phase, and the accounting server is reselected in the accounting phase, which may result in that authentication and accounting for a user is not performed on the same server.

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
```

Related Topics

19.2.9 display radius-server configuration

19.2.25 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.2.26 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.2.20 radius-attribute translate** command to specify the RADIUS attributes that you want to translate.
- Run the **19.2.15 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
```

Related Topics

19.2.20 radius-attribute translate

19.2.44 radius-server template

19.2.27 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*] *

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**]]]

 Copyright © Huawei Technologies Co., Ltd.

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.
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 VPN instance must already exist.
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.
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 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 VRRP6 virtual address.	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 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

To perform RADIUS authentication, configure a RADIUS authentication server in a RADIUS server template. The device uses the RADIUS protocol to communicate

 Copyright © Huawei Technologies Co., Ltd.

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 specify the master/backup algorithm on the RADIUS server and both the primary and secondary authentication servers are configured, the device sends an authentication request packet to the secondary authentication server in either of the following situations:

- The primary authentication server does not send an authentication response packet.
- The authentication request packet retransmission count reaches the maximum.

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
```

Related Topics

19.2.9 display radius-server configuration

19.2.28 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*] } [**ack-reserved-interval** *interval*] [**protect enable**]

undo radius-server authorization { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a RADIUS authorization server.	The value is a unicast address in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authorization server is bound to.	The value is a string of 1 to 31 case-sensitive characters.
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), punctuation mark (.), dash (-), and underline (_). 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 (?). The *key-string* may be a plain text consisting of 1 to 128 characters or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.
ack-reserved-interval *interval*	Specifies the duration for retaining a RADIUS authorization response packet.	The value is an integer that ranges from 0 to 300, in seconds. By default, the value is 0s.
protect enable	Enables the security hardening function.	-
all	Deletes all RADIUS authorization servers.	-

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Specify a RADIUS authorization server.

```
<Huawei> system-view
[Huawei] radius-server authorization 10.1.1.116 shared-key cipher Huawei@2012
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.2.8 display radius-server authorization configuration

19.2.44 radius-server template

19.2.29 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 RADIUS dynamic authorization packet attributes based on global configuration.

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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.2.30 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.2.16 radius-attribute nas-ip** command to configure the NAS-IP-Address attribute in a RADIUS packet sent from an NAS.
     - Run the **19.2.47 radius-server user-name domain-included** command to configure whether the user name carried in the RADIUS packet contains a domain name.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.2.31 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 MAC address format in the calling-station-id attribute carried in RADIUS dynamic authorization packets is xxxxxxxxxxxx, in lowercase.

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

 Copyright © Huawei Technologies Co., Ltd.

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**separator**xx**separator**xx**separator**xx**separator**xx**separator**xx" format.	-
compress	Indicates that the MAC address in the calling-station-id attribute uses the "xxxx**separator**xxxx**separator**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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.2.32 radius-server authorization match-type

Function

The **radius-server authorization match-type** command configures the method used by a device to perform a match check between the RADIUS attribute in the received COA or DM Request packet and user information on the device.

The **undo radius-server authorization match-type** command restores the default setting.

By default, a device performs a match check between the RADIUS attribute in the received COA or DM Request packet and user information on the device using the **any** method, namely, the device performs a match check between a selected attribute in the Request packet and 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 performs a match check between a specified attribute and user information on the device.	-
all	Indicates that the device performs a match check between all attributes and user information on the device.	-

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A device performs a match check between the RADIUS attribute in the COA or DM Request packet and user information on the device to identify users in the following two methods:

- **any** method: The device performs a match check between an attribute and user information on the device. The priority of identifying the RADIUS attributes used by the users is as follows: Acct-Session-ID (4)>Calling-Station-Id (31)>Framed-IP-Address (8) The device searches for the attributes in the Request packet based on the priority, and performs a match check between the first found attribute and 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 performs a match check between all attributes and user information on the device. The device identifies the following RADIUS attributes used by the users: Acct-Session-ID (4), Calling-Station-Id (31), Framed-IP-Address (8), and User-Name (1) The device performs a match check between all the preceding attributes in the Request packet and user information on the device. If all the preceding 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 **19.2.20 radius-attribute translate** command, the match will fail.

Example

Configure a device to perform a match check between all RADIUS attributes in the received COA or DM Request packet and user information on the device.

```
<Huawei> system-view
[Huawei] radius-server authorization match-type all
```

19.2.33 radius-server dead-interval dead-count

Function

The **radius-server dead-interval dead-count** command configures the RADIUS server detection interval and maximum number of consecutive unacknowledged packets in each detection interval.

The **undo radius-server dead-interval dead-count** command restores the default settings.

Format

radius-server { **dead-interval** *dead-interval* | **dead-count** *dead-count* }

undo radius-server { **dead-interval** | **dead-count** }

 Copyright © Huawei Technologies Co., Ltd.

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.

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 multiple RADIUS servers are configured, some servers are Up and the other servers are Down, and the device receives an authentication request packet from a user, the device retransmits the packet to a RADIUS server in Up status based on the server priority and detects the actual status of the server. The following describes the process in which a device detects the status of a RADIUS server.

1. If the device receives no response packet from the RADIUS server and the number of times that the device receives no response packet after sending an authentication request packet is greater than or equal to the maximum number of consecutive unacknowledged packets within the detection interval, the device records a communication interruption.
2. If the device records two consecutive communication interruptions with one RADIUS server, the device considers that the RADIUS server is unavailable and the condition for the device to set the status of the RADIUS server to Down is met.

   NOTE

   If the first connection attempt fails but the second one succeeds, the device deletes the recorded communication interruption with the RADIUS server.
3. When sending an authentication request packet to the RADIUS server again, the device sets the server status to Down. If a response packet is received

 Copyright © Huawei Technologies Co., Ltd.

from the server, the device restores the server status to Up. If no response packet is received from the server and the number of retransmission times is not reached, the device sends an authentication request packet to the server again. If the server still does not respond, the device no longer sends any authentication request packet to the server.

If the device sets the status of all servers that are originally set to Up to Down after the device completes the server status detection based on the preceding detection process or these servers do not respond to the authentication request packets sent from the device, the device sends an authentication request packet to a RADIUS server that is originally set to be Down based on the server priority to detect the server status. (In the original mechanism, the device does not send authentication request packets to the RADIUS servers that are originally set to be Down.)

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.
- To rapidly detect whether the RADIUS server goes Down, when there are a small number of users, smaller values are recommended for the detection interval and maximum number.

Example

Set the RADIUS server detection interval to 10 seconds 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
```

19.2.34 radius-server detect-server interval

Function

The **radius-server detect-server interval** command configures an automatic detection interval for RADIUS servers.

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

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the automatic detection interval for RADIUS servers.	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.

Example

Set the automatic detection interval for RADIUS servers 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
```

19.2.35 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*

undo radius-server format-attribute nas-port

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
nas-port *nas-port-sting*	Specifies the format of the NAS-Port attribute. • The keywords **s**, **t**, **p**, **o**, and **i** stand for 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 be present 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 be present multiple times at any position. They are followed by numbers. For example, **n12** indicates that this position is filled by twelve 1s, and **z12** indicates that this position is filled by 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. • If no VLAN exists, you can add **n** or **z** before **o** or **i** to indicate whether this position	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	is filled by 0s or 1s. That is, **n** and **z** can be followed by numbers or **o/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 by 0s. If **n** is added before **o** or **i**, this field is filled by 1s when no outer VLAN or inner VLAN exists.	

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 yes, 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

 Copyright © Huawei Technologies Co., Ltd.

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. 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 by ten 1s. If the inner VLAN does not exist, this field is filled by 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
```

Related Topics

19.2.38 radius-server nas-port-format

19.2.36 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.

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

 Copyright © Huawei Technologies Co., Ltd.

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 huawei
[Huawei-radius-huawei] radius-server hw-ap-info-format include-ap-ip
```

19.2.37 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 device's hostname.

Format

radius-server nas-identifier-format { **hostname** | **vlan-id** | **ap-info** }

undo radius-server nas-identifier-format

Parameters

Parameter	Description	Value
hostname	Sets the encapsulation format of NAS-Identifier to a 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.	-

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.2.38 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

 Copyright © Huawei Technologies Co., Ltd.

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).	-
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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.2.39 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** | **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.	-

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.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When **new** is specified:

- For Ethernet access users, the NAS port ID format is slot=xx; subslot=xx; port=xxx; VLAN ID=xxxx, in which *slot* ranges from 0 to 15, *subslot* from 0 to 15, *port* from 0 to 255, and *VLAN ID* from 1 to 4094.
- For ADSL access users, the NAS port ID format is slot=xx; subslot=x; port=x;VPI=xxx; VCI=xxxxx, in which *slot* ranges from 0 to 15, *subslot* from 0 to 9, *port* from 0 to 9, *VPI* from 0 to 255, and *VCI* from 0 to 65535.

When **old** is specified:

- For Ethernet access users, the NAS port ID format is slot number (2 characters) + subslot number (2 bytes) + card number (3 bytes) + VLAN ID (9 characters).
- For ADSL access users, the NAS port ID format is slot number (2 characters) + subslot number (2 bytes) + card number (3 bytes) + VPI (8 characters) + VCI (16 characters). A field is prefixed with 0s if its actual value contains fewer characters.

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
```

Related Topics

19.2.9 display radius-server configuration

19.2.40 radius-server retransmit timeout dead-time

Function

The **radius-server retransmit timeout dead-time** command sets the number of times that RADIUS request packets are retransmitted, timeout period, and interval for the server to revert to the active status.

The **undo radius-server retransmit timeout dead-time** command restores the default number of retransmission times, the default timeout period, and the default interval for the server to revert to the active status.

By default, the number of retransmission times is 3, timeout period is 5 seconds, and the interval for the server to revert to the active status is 5 minutes.

Format

radius-server { **retransmit** *retry-times* | **timeout** *time-value* | **dead-time** *dead-time* } *

undo radius-server { **retransmit** [*retry-times*] | **timeout** [*time-value*] | **dead-time** [*dead-time*] } *

 Copyright © Huawei Technologies Co., Ltd.

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 10, in seconds.
dead-time *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

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.

You can run the **radius-server dead-time** *dead-time* command to configure the duration for which the RADIUS server status 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. 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.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If automatic detection for RADIUS servers is configured using the **radius-server testuser** command, the server status is maintained using the automatic detection function. The interval for the RADIUS server to revert to the active status configured using the **radius-server retransmit timeout dead-time** command does not take effect.

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.
- To rapidly detect whether the RADIUS server goes Down, smaller values are recommended for the timeout period and number of retransmission times when there are a small number of users.

Example

Set the number of retransmission times to 3, the timeout period to 2s, and 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 retransmit 3 timeout 2 dead-time 10
```

Related Topics

19.2.9 display radius-server configuration

19.2.44 radius-server template

19.2.41 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**]

 Copyright © Huawei Technologies Co., Ltd.

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 without 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

 Copyright © Huawei Technologies Co., Ltd.

- 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.

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 **Huawei@2012** respectively.

```
<Huawei> system-view
[Huawei] radius-server session-manage 10.1.1.1 shared-key cipher Huawei@2012
```

Related Topics

19.2.11 display radius-server session-manage configuration

19.2.42 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 restores the default shared key of a RADIUS server.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

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.	-

Copyright © Huawei Technologies Co., Ltd.

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

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.

NOTE

To improve security, 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 6 characters.

Example

Set the shared key of a RADIUS server to **Huawei@2012** in cipher text.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server shared-key cipher Huawei@2012
```

Related Topics

19.2.9 display radius-server configuration

19.2.44 radius-server template

 Copyright © Huawei Technologies Co., Ltd.

19.2.43 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.2.42 radius-server shared-key (RADIUS server template view)** 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 6 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 **Huawei@2012**.

```
<Huawei> system-view
[Huawei] radius-server ip-address 10.1.1.1 shared-key cipher Huawei@2012
```

Related Topics

19.2.42 radius-server shared-key (RADIUS server template view)

19.2.44 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*

 Copyright © Huawei Technologies Co., Ltd.

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), punctuation mark (.), underline (_), and hyphens (-).

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 **19.2.21 radius-server (aaa domain view)** 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]
```

Related Topics

19.2.9 display radius-server configuration

19.2.21 radius-server (aaa domain view)

 Copyright © Huawei Technologies Co., Ltd.

19.2.45 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.

 Copyright © Huawei Technologies Co., Ltd.

After automatic detection is configured for users, if the device does not receive authentication packets from the users within the detection interval (configured using the **radius-server detect-server** command), the device performs a RADIUS server detection.

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 and the device sets the RADIUS server status to Up. If the device cannot receive the response packet, the RADIUS server is unavailable and the device sets the RADIUS server status to Down.

Example

Create a user account with the user name **test** and password **Huawei@2012** in RADIUS server template **acs**.

```
<Huawei> system-view
[Huawei] radius-server template acs
[Huawei-radius-acs] radius-server testuser username test password cipher Huawei@2012
```

19.2.46 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.	-

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.2.9 display radius-server configuration

19.2.47 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 RADIUS packets to be 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 the RADIUS server.

The **undo radius-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name when sending RADIUS packets 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 when sending packets to a RADIUS server (applicable to other authentication modes except EAP authentication).

By default, the device does not modify the user name entered by the user in the packets sent to the RADIUS server.

Format

radius-server user-name domain-included

 Copyright © Huawei Technologies Co., Ltd.

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 when sending RADIUS packets to a RADIUS server.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] undo radius-server user-name domain-included
```

Related Topics

19.2.9 display radius-server configuration

19.2.48 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.2.7 display radius-server accounting-stop-packet

 Copyright © Huawei Technologies Co., Ltd.

19.2.49 snmp-agent trap enable feature-name radius

Function

The **snmp-agent trap enable feature-name radius** command enables the trap function for the RDS module.

The **undo snmp-agent trap enable feature-name radius** command disables the trap function for the RDS module.

By default, the trap function is disabled for the RDS module.

Format

snmp-agent trap enable feature-name radius [**trap-name** { **hwradiusacctserverdown** | **hwradiusacctserverup** | **hwradiusauthserverdown** | **hwradiusauthserverup** }]

undo snmp-agent trap enable feature-name radius [**trap-name** { **hwradiusacctserverdown** | **hwradiusacctserverup** | **hwradiusauthserverdown** | **hwradiusauthserverup** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event of the RDS module.	-
hwradiusacctserver-down	Enables the device to send a Huawei proprietary trap when it detects that communication with the RADIUS accounting server is interrupted.	-
hwradiusacctserverup	Enables the device to send a Huawei proprietary trap when it detects that communication with the RADIUS accounting server is restored.	-
hwradiusauthserver-down	Enables the device to send a Huawei proprietary trap when it detects that communication with the RADIUS authentication server is interrupted.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwradiusauthserverup	Enables the device to send a Huawei proprietary trap when it detects that communication with the RADIUS authentication server is restored.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** to enable the trap function for one or more events.

Example

Enable the trap function for hwradiusacctserverdown of the RDS module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name radius trap-name hwradiusacctserverdown
```

Related Topics

19.2.13 display snmp-agent trap feature-name radius all

19.2.50 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** | **accounting** [**start** | **realtime** | **stop**]]

 Copyright © Huawei Technologies Co., Ltd.

test-aaa *user-name user-password* **hwtacacs-template** *template-name* [**accounting** [**start** | **realtime** | **stop**]]

Parameters

Parameter	Description	Value
user-name	Specifies a user name.	The value is a string of 1 to 253 case-insensitive characters. **NOTE** When the HWTACACS, or RADIUS server is detected, the user name cannot contain spaces.
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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
accounting	Indicates accounting. By default, an accounting-start packet is sent.	-
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.

Prerequisites

An authentication server template or accounting server template has been created, an authentication server or accounting server has been specified in the

 Copyright © Huawei Technologies Co., Ltd.

authentication server template or accounting server template, and 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 authentication server 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 authentication server.

Precautions

chap and **pap** are two authentication modes.

- 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 **huawei**.

```
<Huawei> test-aaa user1 userkey radius-template huawei chap
Info: The server template does not exist.
```

19.2.51 radius-server dead-detect-condition by-server-ip

Function

The **radius-server dead-detect-condition by-server-ip** command configures keepalive detection for RADIUS server based on the RADIUS server IP address.

The **undo radius-server dead-detect-condition by-server-ip** command restores the default setting.

By default, keepalive detection is performed for only RADIUS authentication server.

Format

radius-server dead-detect-condition by-server-ip

 Copyright © Huawei Technologies Co., Ltd.

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.

When detecting the Down states of RADIUS authentication and accounting servers, the device counts the numbers of authentication and accounting request packets separately. 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 keepalive detection for RADIUS server based on RADIUS server IP address.

```
<Huawei> system-view
[Huawei] radius-server dead-detect-condition by-server-ip
```

 Copyright © Huawei Technologies Co., Ltd.

19.3 HWTACACS Configuration Commands

19.3.1 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	Displays information about Accounting-Stop packets starting from a specified number.	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

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

During HWTACACS troubleshooting, you can run this command to check information about Accounting-Stop packets sent by the HWTACACS server.

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 19-32 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.

Related Topics

19.3.7 hwtacacs-server accounting-stop-packet resend

19.3.20 reset hwtacacs-server accounting-stop-packet

19.3.2 display hwtacacs-server template

Function

The **display hwtacacs-server template** command displays the configurations of an HWTACACS server template.

Format

display hwtacacs-server template [*template-name*]

 Copyright © Huawei Technologies Co., Ltd.

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 configuration of HWTACACS server templates and isolate 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 all HWTACACS server templates.

```
<Huawei> display hwtacacs-server template
 ------------------------------------------------------------------------------
 Global:
 Shared-key                    : **********
 ------------------------------------------------------------------------------
 HWTACACS-server template name   : template0
 Primary-authentication-server   : 192.168.18.102:49 Vrf:- Shared-key:- Status:UP
 Primary-authorization-server    : 192.168.18.102:49 Vrf:- Shared-key:* Status:UP
 Primary-accounting-server       : 192.168.18.102:49 Vrf:- Shared-key:* Status:UP
 Secondary-authentication-server : -:0 Vrf:- Shared-key:- Status:-
 Secondary-authorization-server  : -:0 Vrf:- Shared-key:- Status:-
 Secondary-accounting-server     : -:0 Vrf:- Shared-key:- Status:-
 Third-authentication-server     : -:0 Vrf:- Shared-key:- Status:-
 Third-authorization-server      : -:0 Vrf:- Shared-key:- Status:-
 Third-accounting-server         : -:0 Vrf:- Shared-key:- Status:-
 Current-authentication-server   : 192.168.18.102:49 Vrf:- Shared-key:- Status:UP
 Current-authorization-server    : 192.168.18.102:49 Vrf:- Shared-key:* Status:UP
 Current-accounting-server       : 192.168.18.102:49 Vrf:- Shared-key:* Status:UP
 Source-IP-address               : -
 Source-LoopBack                 : -
 Source-IPv6-address             : -
 IPv6 Source-LoopBack            : -
 Shared-key                    : -
 Quiet-interval(min)             : 5
 Response-timeout-Interval(sec)  : 5
 Domain-included                 : NO
 Traffic-unit                  : B
 ------------------------------------------------------------------------------
 Total 2,2 printed
```

Display the configuration of the HWTACACS server template **template0**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display hwtacacs-server template template0
-------------------------------------------------------------------------------
HWTACACS-server template name   : template0
Primary-authentication-server   : FC00::2:1:20 Vrf:- Shared-key:- Status:UP
Primary-authorization-server    : -:0 Vrf:- Shared-key:- Status:-
Primary-accounting-server       : -:0 Vrf:- Shared-key:- Status:-
Secondary-authentication-server : 10.1.1.1:20 Vrf:- Shared-key:* Status:UP
Secondary-authorization-server  : -:0 Vrf:- Shared-key:- Status:-
Secondary-accounting-server     : 10.1.1.1:10 Vrf:- Shared-key:* Status:UP
Third-authentication-server     : -:0 Vrf:- Shared-key:- Status:-
Third-authorization-server      : -:0 Vrf:- Shared-key:- Status:-
Third-accounting-server         : -:0 Vrf:- Shared-key:- Status:-
Current-authentication-server   : FC00::2:1:20 Vrf:- Shared-key:- Status:UP
Current-authorization-server    : -:0 Vrf:- Shared-key:- Status:-
Current-accounting-server       : 10.1.1.1:10 Vrf:- Shared-key:* Status:UP
Source-IP-address               : -
Source-LoopBack                 : -
Source-IPv6-address             : -
IPv6 Source-LoopBack            : -
Shared-key                      : -
Quiet-interval(min)             : 5
Response-timeout-Interval(sec)  : 5
Domain-included                 : Original
Traffic-unit                    : B
-------------------------------------------------------------------------------
```

Table 19-33 Description of the **display hwtacacs-server template** command output

Item	Description
Global	Global configuration information.
HWTACACS-server template name	Name of the HWTACACS server template.
Primary-authentication-server	IP address, port number, VPN instance, shared key, and status of the primary authentication server.
Primary-authorization-server	IP address, port number, VPN instance, shared key, and status of the primary authorization server.
Primary-accounting-server	IP address, port number, VPN instance, shared key, and status of the primary accounting server.
Secondary-authentication-server	IP address, port number, VPN instance, shared key, and status of the second authentication server.
Secondary-authorization-server	IP address, port number, VPN instance, shared key, and status of the second authorization server.
Secondary-accounting-server	IP address, port number, VPN instance, shared key, and status of the second accounting server.
Third-authentication-server	IP address, port number, VPN instance, shared key, and status of the third authentication server.
Third-authorization-server	IP address, port number, VPN instance, shared key, and status of the third authorization server.
Third-accounting-server	IP address, port number, VPN instance, shared key, and status of the third accounting server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current-authentication-server	IP address, port number, VPN instance, shared key, and status of the authentication server in use.
Current-authorization-server	IP address, port number, VPN instance, shared key, and status of the authorization server in use.
Current-accounting-server	IP address, port number, VPN instance, shared key, and status of the accounting server in use.
Source-IP-address	Source IP 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.
Shared-key	The first Shared-key indicates the shared key of the HWTACACS server configured in the system view. The second Shared-key indicates the shared key of the HWTACACS server configured in the HWTACACS server template view.
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.
Total 1,1 printed	Total number of HWTACACS server templates and number of printed HWTACACS server templates.

19.3.3 display hwtacacs-server template verbose

Function

The **display hwtacacs-server template verbose** command displays statistics on HWTACACS authentication, accounting, and authorization.

 Copyright © Huawei Technologies Co., Ltd.

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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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:
```

 Copyright © Huawei Technologies Co., Ltd.

```
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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-34 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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• HWTACACS account client round trip time(s): Response time of the last accounting packet of the HWTACACS server

19.3.4 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] undo hwtacacs enable
```

19.3.5 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 **19.3.14 hwtacacs-server template** command.

Example

Apply the HWTACACS server template **tacacs1** to the domain **tacacs1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<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
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 hwtacacs-server template

19.3.6 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* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third**] [**shared-key cipher** *key-string*]

hwtacacs-server accounting *ipv6-address* [*port*] [**public-net**] [**secondary** | **third**] [**shared-key cipher** *key-string*]

undo hwtacacs-server accounting [**secondary** | **third**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS accounting server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of the 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 VPN instance must already exist.
secondary	Configures the second HWTACACS accounting server as the standby server. If no standby 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
shared-key cipher *key-string*	Indicates the shared key of the specified HWTACACS accounting server.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: • Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. • Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

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

 Copyright © Huawei Technologies Co., Ltd.

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 type (for example, the servers are all primary servers), only the latest configuration takes effect.

Example

Configure the shared key of the primary HWTACACS accounting server to **Admin@123**.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server accounting 10.163.155.12 52 shared-key cipher Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.7 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.3.1 display hwtacacs-server accounting-stop-packet

19.3.8 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* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third**] [**shared-key cipher** *key-string*]

 Copyright © Huawei Technologies Co., Ltd.

hwtacacs-server authentication *ipv6-address* [*port*] [**public-net**] [**secondary** | **third**] [**shared-key cipher** *key-string*]

undo hwtacacs-server authentication [**secondary** | **third**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS authentication server.	The value is a valid unicast address in dotted decimal notation.
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.
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 accounting server is bound to.	The VPN instance must already exist.
secondary	Configures the second HWTACACS authentication server as the standby server. If no standby server is configured, the primary HWTACACS authentication server is specified.	-
third	Configures the third HWTACACS authentication server as the standby server. If no secondary server is configured, the primary HWTACACS authentication server is specified.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
shared-key cipher *key-string*	Indicates the shared key of the specified HWTACACS authentication server.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: • Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. • Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

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

 Copyright © Huawei Technologies Co., Ltd.

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 type (for example, the servers are all primary servers), only the latest configuration takes effect.

Example

Configure the shared key of the primary HWTACACS authentication server to **Admin@123**.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server authentication 10.163.155.12 49 shared-key cipher Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.9 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* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third**] [**shared-key cipher** *key-string*]

hwtacacs-server authorization *ipv6-address* [*port*] [**public-net**] [**secondary** | **third**] [**shared-key cipher** *key-string*]

undo hwtacacs-server authorization [**secondary** | **third**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS authorization server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of the 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 VPN instance must already exist.
secondary	Configures the second HWTACACS authorization server as the standby server. If no standby server is configured, the primary HWTACACS authorization server is specified.	-
third	Configures the third HWTACACS authorization server as the standby server. If no secondary server is configured, the primary HWTACACS authorization server is specified.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
shared-key cipher *key-string*	Indicates the shared key of the specified HWTACACS authorization server.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: • Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. • Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 type (for example, the servers are all primary servers), only the latest configuration takes effect.

Example

Configure the shared key of the primary HWTACACS authorization server to **Admin@123**.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server authorization 10.163.155.12 49 shared-key cipher Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.10 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
key-string	Specifies a shared key.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: • Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. • Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

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

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 6 characters.

You can modify this configuration only when the HWTACACS server template is not in use.

To be compatible with the earlier versions, the device supports the shared key of 20 characters in cipher text. The length of the shared key cannot be configured.

Example

Set the shared key of the HWTACACS server to **Admin@123**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server shared-key cipher Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 hwtacacs-server template

19.3.11 hwtacacs-server shared-key (system view)

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	Indicates the shared key of the HWTACACS server.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: • Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. • Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

Copyright © Huawei Technologies Co., Ltd.

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 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.

You can run the **19.3.10 hwtacacs-server shared-key** command in the HWTACACS server template view to configure the shared keys. However, after this command is run, all HWTACACS servers in the template use the same shared key. To configure shared keys for different HWTACACS servers, run the **19.3.8 hwtacacs-server authentication**, **19.3.9 hwtacacs-server authorization**, and **19.3.6 hwtacacs-server accounting** commands.

If no shared key is configured in the HWTACACS server template, run the **hwtacacs-server shared-key** command in the system view to configure it. The shared key configured in the system view is valid for all HWTACACS server templates.

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 6 characters.

To be compatible with the earlier versions, the device supports the shared key of 20 characters in cipher text. The length of the shared key cannot be configured.

The HWTACACS shared keys are used in the following order:

1. Shared key of the HWTACACS authentication, authorization, and accounting server with the specified IP address configured in the HWTACACS server template view
2. Shared key of the HWTACACS server configured in the HWTACACS server template view
3. Shared key of the HWTACACS server configured in the system view
4. If there is no available shared key of HWTACACS server, the system considers that the operation failed.

Example

Set the shared key of the HWTACACS server to **Admin@123**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] hwtacacs-server shared-key cipher Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.12 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*

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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 hwtacacs-server template

19.3.13 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*

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.
source-loopback *interface-number*	Configures a loopback interface as the source IPv6 address for communicating with the HWTACACS server.	The loopback interface must already exist.

Views

HWTACACS server template view

 Copyright © Huawei Technologies Co., Ltd.

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.

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
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 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 --.

Copyright © Huawei Technologies Co., Ltd.

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 **19.3.5 hwtacacs-server** command in the domain view to apply the HWTACACS server template.

Precautions

You can modify the content of a template or 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]
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.5 hwtacacs-server

19.3.15 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*

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] hwtacacs-server template template1
[Huawei-hwtacacs-template1] hwtacacs-server timer quiet 3
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.16 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 hwtacacs-server template

19.3.17 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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
```

Related Topics

19.3.2 display hwtacacs-server template
19.3.14 hwtacacs-server template

19.3.18 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.3.2 display hwtacacs-server template

 Copyright © Huawei Technologies Co., Ltd.

19.3.19 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

 Copyright © Huawei Technologies Co., Ltd.

before the passwords expire. If a user needs to run this command to change the passwords of other users, the user must have the system rights.

Example

Enable the user that passes HWTACACS authentication to change the password.

```
<Huawei> hwtacacs-user change-password hwtacacs-server huawei
Username:cj@huawei
Old Password:
New Password:
Re-enter New password:
Info: The password has been changed successfully.
```

19.3.20 reset hwtacacs-server accounting-stop-packet

Function

The **reset hwtacacs-server accounting-stop-packet** command clears statistics on the remaining buffer information of HWTACACS accounting-stop packets.

Format

reset hwtacacs-server accounting-stop-packet { **all** | **ip** { *ipv4-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Clears statistics on the remaining buffer information of HWTACACS 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 remaining buffer 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

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command can clear statistics on the remaining buffer information of HWTACACS accounting-stop packets. The deleted statistics cannot be restored.

Example

Clear statistics on the remaining buffer information of all HWTACACS accounting-stop packets.

```
<Huawei> reset hwtacacs-server accounting-stop-packet all
```

Related Topics

19.3.1 display hwtacacs-server accounting-stop-packet

19.3.21 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.3.2 display hwtacacs-server template

19.4 HACA Configuration Commands

19.4.1 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

 Copyright © Huawei Technologies Co., Ltd.

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 19-35 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.

Related Topics

19.4.6 haca-server accounting-stop-packet resend

19.4.17 reset haca-server accounting-stop-packet all

19.4.2 display haca-server configuration

Function

The **display haca-server configuration** command displays the configurations of HACA server templates.

Format

display haca-server configuration [**template** *template-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
template *template-name*	Specifies the name of an HACA server template. If this parameter is not specified, the configuration of all the HACA server templates is displayed.	The HACA server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display haca-server configuration** command output helps you check the configuration of HACA server templates or troubleshoot HACA.

Example

Display the configurations of HACA server templates.

```
<Huawei> display haca-server configuration
  ------------------------------------------------------------------------------
  HACA-server template name                 : haca
  HACA-server server-ip-address(port)       : 10.22.85.246(50300)
  HACA-server pki-realm-name                : default
  HACA-server Status                      : REGISTE
  HACA-server source-ip-address           : -
  HACA-server down-delay-interval(sec)      : 30
  HACA-server response-timeout-interval(sec) : 5
  HACA-server domain-included               : ORIGINAL
  HACA-server heart-beat-interval(min)      : 20
  HACA-server reconnection-interval(min)    : 1
  HACA-server user-syn-interval(min)        : 9
  HACA-server server-escape-state           : 0
  HACA-server accounting-stop-packet resend  : 3
  ------------------------------------------------------------------------------
  Total 1,1 printed
```

Table 19-36 Description of the **display haca-server configuration** command output

Item	Description
HACA-server template name	Name of the HACA server template. To create an HACA server template, run the **haca-server template** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
HACA-server server-ip-address(port)	IP address and port number of the HACA server. To set the IP address and port number for the HACA server, run the **19.4.7 haca-server server-address** command.
HACA-server pki-realm-name	Name of a PKI domain of the HACA server. To set the name of a PKI domain of the HACA server, run the **19.4.7 haca-server server-address** command.
HACA-server Status	Status of the HACA server. The values are as follows: • IDLE: indicates the idle state. • INIT: indicates the initial state. • UP: indicates the UP state. • REGISTE: indicates the registration state. • DOWN: indicates the DOWN state.
HACA-server source-ip-address	Source IP address of HACA packets. To set the source IP address of HACA packets, run the **19.4.8 haca-server source-ip** command.
HACA-server down-delay-interval(sec)	Delay interval for HACA server to restart from the DOWN state, in seconds. To set the delay interval, run the **19.4.10 haca-server timer down-delay** command.
HACA-server response-timeout-interval(sec)	Timeout period for the HACA server to send reply packets, in seconds. To set the timeout period, run the **19.4.13 haca-server timer response-timeout** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
HACA-server domain-included	Format of HACA user name. It specifies whether the user name sent to the HACA server contains a domain name. • YES: indicates that the user name contains the domain name. • NO: indicates that the user name does not contain the domain name. • ORIGINAL: indicates that the device does not modify the user name entered by the user. To set the user name format, run the **19.4.15 haca-server user-name** command.
HACA-server heart-beat-interval(min)	Interval for the HACA server to send heartbeat packets, in minutes. To set the heartbeat interval, run the **19.4.11 haca-server timer heart-beat** command.
HACA-server reconnection-interval(min)	Interval for the HACA server to be reconnected, in minutes. To set the reconnection interval, run the **19.4.12 haca-server timer reconnection** command.
HACA-server user-syn-interval(min)	Interval for synchronizing HACA user information, in minutes. To set the synchronization interval, run the **19.4.14 haca-server timer user-syn** command.
HACA-server server-escape-state	Escape state of HACA. • 0: indicates that the server is in the UP state, and the best-effort path will not be used. • 1: indicates that the server is in the DOWN state, and the best-effort path is being prepared. • 2: indicates that the server is in the initial state, and the best-effort path will not be used.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
HACA-server accounting-stop-packet resend	Number of times HACA accounting-stop packets are retransmitted. To set the number of times HACA accounting-stop packets can be retransmitted, run the **19.4.6 haca-server accounting-stop-packet resend** command.

19.4.3 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 19-37 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

19.4.4 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

haca enable

undo haca enable

Parameters

None

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the cloud management scenario, users are authenticated through Portal. 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 **19.4.7 haca-server server-address** command.

Example

Enable HACA.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei] haca-server server-address 10.1.1.1 default
[Huawei-haca-haca] haca enable
```

19.4.5 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **huawei**.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] quit
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] haca-server haca
```

19.4.6 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

You can modify the configuration only when the HACA server template is not in use.

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
```

19.4.7 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.

 Copyright © Huawei Technologies Co., Ltd.

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*

undo haca-server server-address [*ip-address* [*port*]]

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.
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.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

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.

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 default
```

 Copyright © Huawei Technologies Co., Ltd.

19.4.8 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
```

 Copyright © Huawei Technologies Co., Ltd.

19.4.9 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 **19.4.5 haca-server (AAA domain view)** in the domain view to apply the HACA server template.

 Copyright © Huawei Technologies Co., Ltd.

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]
```

19.4.10 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.4.11 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.4.12 haca-server timer reconnection

Function

The **haca-server timer reconnection** command sets the reconnection interval for an HACA server.

The **undo haca-server timer down-detection** 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.4.13 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] haca-server timer response-timeout 30
```

19.4.14 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the user information synchronization interval for the HACA server to 30 minutes.

```
<Huawei> system-view
[Huawei] haca-server timer user-syn 30
```

19.4.15 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 to be 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

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

 Copyright © Huawei Technologies Co., Ltd.

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.

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
```

19.4.16 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-syn	Clears all HACA user synchronization information.	-
cut-notify	Clears all HACA logout notifications.	-
cut-request	Clears all HACA logout requests.	-
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 **19.4.3 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
```

Related Topics

19.4.3 display haca-server statistics

19.4.17 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.4.1 display haca-server accounting-stop-packet all

19.5 DAA Configuration Commands

19.5.1 acl tariff-level

Function

The **acl tariff-level** command configures a tariff level for traffic.

The **undo acl tariff-level** command deletes the tariff level.

By default, no tariff level is configured.

Format

acl *acl-number* **tariff-level** *tariff-level*

undo acl *acl-number* **tariff-level**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999.
tariff-level	Specifies the tariff level.	The value is an integer that ranges from 1 to 2.

Views

Traffic group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On a network where users need to pay for the network access service, such as a campus network, users are not charged when they access internal network resources, and are charged when they access the Internet resources. Therefore, the device must be able to know whether the user traffic goes to the internal network or Internet according to the destination IP addresses of the traffic.

After distinguishing the traffic, the device uses the tariff level specified for the traffic and the corresponding accounting policy to offer differentiated services. This command is used to specify the tariff levels for different traffic.

Prerequisites

An IPv4 ACL must have been created using the **19.7.4 acl (system view)** or **19.7.3 acl name** command.

Precautions

- In the ACL rule, the destination address (the **destination** parameter) is mandatory, and the source address (the **source** parameter) is optional. Configuring both the source and destination addresses can precisely specify the traffic on which accounting will be performed.
- If there is an ACL rule with both the source and destination addresses configured and the destination address is the same as that in another ACL rule, you are advised to match this ACL rule with a tariff level (*tariff-level*) with a small value during configuration. For example, most users accessing destination address A on the network use the same tariff corresponding to ACL 3000, and a small number of users with source address B and accessing destination address A use another tariff corresponding to ACL 3001. In this case, the tariff level corresponding to ACL 3001 should have a smaller value than the tariff level corresponding to ACL 3000.

 Copyright © Huawei Technologies Co., Ltd.

- If the **any** parameter is specified, the device does not check the source and destination addresses of packets, and considers that all packets match the ACL rule. The device then executes the corresponding action.

Example

Configure tariff level 1 for the traffic matching ACL 3000.

```
<Huawei> system-view
[Huawei] acl number 3000
[Huawei-acl-adv-3000] rule 5 permit ip source any destination 10.0.0.1 0.0.0.255
[Huawei-acl-adv-3000] quit
[Huawei] traffic-group p1
[Huawei-traffic-group-p1] acl 3000 tariff-level 1
```

Related Topics

19.5.2 display traffic-group

19.5.2 display traffic-group

Function

The **display traffic-group** command displays information about traffic groups.

Format

display traffic-group { **all** | **name** *group-name* }

Parameters

Parameter	Description	Value
all	Displays information about all traffic groups.	-
name *group-name*	Displays detailed information about a specified traffic group.	The traffic group name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display traffic-group** command displays information about traffic groups.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about all traffic groups.

```
<Huawei> display traffic-group all
--------------------------------------------------------------------------------
ID   Traffic-group-name             Rule-num   Tariff-level-num  Status
--------------------------------------------------------------------------------
1    huawei                         1          1                 disable
--------------------------------------------------------------------------------
Total: 1
```

Table 19-38 Description of the display traffic-group all command output

Item	Description
ID	Traffic group ID.
Traffic-group-name	Name of the traffic group. To configure a traffic group, run the **19.5.4 traffic-group** command.
Rule-num	Number of ACL rules in a traffic group.
Tariff-level-num	Number of tariff levels in a traffic group.
Status	Status of a traffic group: • enable: Traffic group is enabled. • disable: Traffic group is disabled. To apply a traffic group, run the **19.5.5 traffic-group enable** command.
Total	Number of traffic groups.

Display details about the traffic group **huawei**.

```
<Huawei> display traffic-group name huawei
--------------------------------------------------------------------------------
Acl-id              Tariff-level
--------------------------------------------------------------------------------
3000                   1
--------------------------------------------------------------------------------
Total: 1
```

Table 19-39 Description of the display traffic-group name command output

Item	Description
Acl-id	ACL rule that identifies traffic. To specify an ACL rule, run the **19.5.1 acl tariff-level** command.
Tariff-level	Tariff level of traffic. To configure a tariff level, run the **19.5.1 acl tariff-level** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Total	Number of ACL rules in a traffic group.

Related Topics

19.5.4 traffic-group

19.5.1 acl tariff-level

19.5.5 traffic-group enable

19.5.3 tariff-level

Function

The **tariff-level** command configures the QoS profile and accounting function for a tariff level.

The **undo tariff-level** command restores the default configuration.

By default, the QoS profile and accounting function are not configured for tariff levels.

Format

tariff-level *tariff-level* { **qos-profile** *profile-name* | **accounting-on** } *

undo tariff-level *tariff-level* [**qos-profile** | **accounting-on**]

Parameters

Parameter	Description	Value
tariff-level	Specifies the tariff level.	The value is an integer that ranges from 1 to 2.
qos-profile *profile-name*	Specifies the name of the QoS profile corresponding to the tariff level.	The QoS profile name must already exist.
accounting-on	Enables accounting for the tariff level.	-

Views

AAA domain view, service scheme view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After the tariff level is configured for classified traffic, you need to configure the QoS profile and accounting function for the tariff level to implement destination-based accounting. The QoS profile is used to collect traffic statistics based on destination addresses. After the accounting function is enabled, the device can send statistics to the RADIUS accounting server.

The DAA policy priorities on the device are as follows: DAA policy in a service scheme delivered by the RADIUS server > DAA policy in a service scheme bound to a domain > DAA policy configured in a domain.

To delete a DAA policy, it is recommended that you make users go offline first and make them go online after deleting the DAA policy.

Prerequisites

The QoS profile has been created using the **20.3.18 qos-profile** command.

Example

Configure the QoS profile huawei for tariff level 1 and enable the accounting function.

```
<Huawei> system-view
[Huawei] qos-profile huawei
[Huawei-qos-profile-huawei] statistics enable
[Huawei-qos-profile-huawei] quit
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] tariff-level 1 qos-profile huawei accounting-on
```

Related Topics

19.1.41 display domain

20.3.18 qos-profile

19.5.4 traffic-group

Function

The **traffic-group** command creates a traffic group and displays the traffic group view, or displays the view of an existing traffic group.

The **undo traffic-group** command deletes a traffic group.

By default, no traffic group exists on the device.

Format

traffic-group *group-name*

undo traffic-group *group-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Indicates the name of a traffic group.	The value is a string of 1 to 31 case-sensitive characters. It cannot be - or -- and cannot contain spaces or the following symbols: / \ : < > | @ ' % * " ?.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By using the traffic group, the device can identify the traffic going to different destination addresses, apply different tariff levels for the traffic, and enforce different accounting policies.

Follow-up Procedure

- After a traffic group is created, the traffic group view is displayed. Run the **19.5.1 acl tariff-level** command in the traffic group view to configure a tariff level.
- Run the **19.5.5 traffic-group enable** command in the system view to make the traffic group effective.

Precautions

The device supports a maximum of 8 traffic groups.

Example

Create the traffic group p1.

```
<Huawei> system-view
[Huawei] traffic-group p1
```

Related Topics

19.5.2 display traffic-group

 Copyright © Huawei Technologies Co., Ltd.

19.5.5 traffic-group enable

Function

The **traffic-group enable** command applies a traffic group to the device globally.

The **undo traffic-group enable** command restores the default configuration.

By default, no traffic group is applied to the device.

Format

traffic-group *group-name* **enable**

undo traffic-group *group-name* **enable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a traffic group that you want to apply to the device.	The traffic group name must already exist.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The traffic group takes effect for users only after it is globally applied to the device.

Prerequisites

The traffic group has been created using the **19.5.4 traffic-group** command.

Precautions

- Only one traffic group can be applied to the device globally.
- If you run this command multiple times, only the latest configuration takes effect.
- If you modify a traffic group that has been applied, the modification takes effect only after the traffic group is applied to the device again by using this command.

Copyright © Huawei Technologies Co., Ltd.

- The **19.5.1 acl tariff-level** command changes the tariff level of traffic.
- The **19.7.16 rule (advanced ACL view)** command changes the source or destination address in the traffic classification rule.

Example

Apply the traffic group p1 to the device globally.

```
<Huawei> system-view
[Huawei] traffic-group p1
[Huawei-traffic-group-p1] quit
[Huawei] traffic-group p1 enable
```

Related Topics

19.5.2 display traffic-group

19.6 NAC Configuration Commands

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support NAC.

19.6.1 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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

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 **19.1.50 domain (AAA view)** command in the AAA view.

 Copyright © Huawei Technologies Co., Ltd.

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 **huawei** in the authentication profile **p1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] quit
[Huawei-aaa] quit
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] access-domain huawei force
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.2 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*

 Copyright © Huawei Technologies Co., Ltd.

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.
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.

You can set source addresses of offline detection packets for users in a maximum of 1024 VLANs.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 2222-1111-1234
```

19.6.3 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 255.255.255.255.

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

 Copyright © Huawei Technologies Co., Ltd.

- This function does not take effect for users who use Layer 3 Portal authentication.
- 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.

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
```

19.6.4 access-user acl-priviledge-revert

Function

The **access-user acl-priviledge-revert** command configures the device to match packets with ACL rules in ascending order by rule IDs. That is, a smaller rule ID indicates a higher priority of the rule.

The **undo access-user acl-priviledge-revert** command restores the default matching sequence for ACL rules.

By default, the device matches packets with ACL rules in descending order by rule IDs. That is, a larger rule ID indicates a higher priority of the rule.

Format

access-user acl-priviledge-revert

undo access-user acl-priviledge-revert

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

By default, the device matches packets with ACL rules in descending order by rule IDs. You can use the **access-user acl-priviledge-revert** command to configure the device to match packets with ACL rules in ascending order by rule IDs.

Precautions

The configuration takes effect only after the device is restarted.

Example

Configure the device to match packets with ACL rules in ascending order by rule IDs.

```
<Huawei> system-view
[Huawei] access-user acl-priviledge-revert
```

19.6.5 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 ACLs bound to a user group.	-

Views

User group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After creating a user group using the **19.6.150 user-group** command, you can run the **acl-id** command to bind an ACL to the user group. The device will deliver ACL rules based on the user group and the ACL rules apply to all users in the user group.

Prerequisites

The ACL to be bound to a user group must have been created using the **19.7.4 acl (system view)** command.

Precautions

- If a user group contains online users, the ACL bound to the 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, add an ACL rule that denies all network access and ensure that the ACL rule takes effect.
- To grant the same network access rights to all users in a user group, do not configure the source IP address in an ACL rule bound to the user group. If an ACL rule defines the source IP address, only users whose IP address is the source IP address match the ACL rule.

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
```

Related Topics

19.6.51 display user-group

19.6.6 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.

 Copyright © Huawei Technologies Co., Ltd.

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 invalid 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 (set using the **19.6.16 authentication timer handshake-period** command), the device deletes the user entry.

Precautions

- All pre-connection users support this function. Among users who fail to be authenticated or pass authentication, only MAC address authentication users, and 802.1X authentication users support this function. The offline detection function for Portal authentication users is configured using the **portal timer offline-detect** command.
- This function takes effect only for the wired users who obtain IP addresses.
- 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.

Example

In the authentication profile **p1**, enable the handshake with pre-connection users and authorized users.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] authentication handshake
```

19.6.7 authentication authen-fail fail-times

Function

The **authentication authen-fail fail-times** command configures the maximum number of consecutive authentication failures.

The **undo authentication authen-fail** command restores the default maximum number of consecutive authentication failures.

By default, the maximum number of consecutive authentication failures is 1.

Format

authentication authen-fail fail-times *fail-times*

undo authentication authen-fail

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of consecutive authentication failures.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Users may fail to pass authentication due to reasons such as temporary unreachability of the server. To improve authentication reliability, you can configure the maximum number of consecutive authentication failures so that users can be re-authenticated after an authentication failure within the allowed range. If the number of consecutive authentication failures exceeds the maximum value, the authentication fails.

Example

Set the maximum number of consecutive authentication failures to 2.

```
<Huawei> system-view
[Huawei] authentication authen-fail fail-times 2
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.8 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
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.9 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* }

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* } [**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* } [**response-fail**]

undo authentication event authen-server-down 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.	-
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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.	-
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.

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 the client, configure authentication event

 Copyright © Huawei Technologies Co., Ltd.

authorization information. The device will assign network access rights to these users based on the authentication phase.

Precautions

Wireless 802.1X authentication does not support this function.

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.

Only the 8FE1GE, 24GE, and 24ES2GP cards, and the AR2201-48FE and AR2202-48FE support the delivery of authorized VLANs to users.

VLAN-based authorization does not apply to the authentication users who access through VLANIF interfaces.

An authorized VLAN cannot be delivered to online Portal users.

This function takes effect only for users who go online after this function is successfully configured.

When the authentication server is in Down state, user authentication fails, or the user is in pre-connection state, the redirection ACL function is not supported.

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.

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
```

19.6.10 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **19.2.45 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] authentication-profile name authen1
[Huawei-authen-profile-authen1] authentication event authen-server-up action re-authen
```

19.6.11 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* | **user-group** *user-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.
user-group *user-group-name*	Specifies the name of a user group based on which network access rights are assigned.	The value must be an existing user 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

 Copyright © Huawei Technologies Co., Ltd.

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

Only the 8FE1GE, 24GE, and 24ES2GP cards, and the AR2201-48FE and AR2202-48FE support the delivery of authorized VLANs to users.

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 redirection ACL function is not supported.

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
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.12 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

authentication event portal-server-down action authorize user-group *user-group-name*

undo authentication event portal-server-down action authorize

Parameters

Parameter	Description	Value
user-group *user-group-name*	Specifies the name of the user group based on which network access rights are assigned to users.	The value must be an existing user 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 user group has been created using the **user-group** command in the system view.

Precautions

- This function takes effect only for users who go online after this function is successfully configured.
- Only HTTP 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 redirection ACL function is not supported.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the Portal access profile **p1**, configure the device to assign network access rights based on the user group **g1** to users when the Portal server is Down.

```
<Huawei> system-view
[Huawei] user-group g1
[Huawei-user-group-g1] quit
[Huawei] portal-access-profile name p1
[Huawei-portal-acces-profile-p1] authentication event portal-server-down action authorize user-group g1
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.13 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-

 Copyright © Huawei Technologies Co., Ltd.

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-acces-profile-p1] authentication event portal-server-up action re-authen
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.14 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 disabled.

Format

authentication ip-address in-accounting-start

undo authentication ip-address in-accounting-start

Parameters

None

Views

Authentication profile view

 Copyright © Huawei Technologies Co., Ltd.

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.

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
```

19.6.15 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.16 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 that ranges from 5 to 7200, in seconds.

Views

Authentication profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the handshake with pre-connection users and authorized users using the **19.6.6 authentication handshake** command, you can run the this 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

- All pre-connection users support this function. Among users who fail to be authenticated or pass authentication, only MAC address authentication users, and 802.1X authentication users support this function. The offline detection function for Portal authentication users is configured using the **portal timer offline-detect** command.
- This function takes effect only for the wired users who obtain IP addresses. By default, wired users without IP addresses go offline after 30 minutes.
- 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.
- If the configured handshake interval is less than the default value, an IP address conflict may occur between terminal detection and device ARP probe. For example, a Windows client sends a detection packet with the source address 0.0.0.0 at an interval of 10 seconds after obtaining an IP address. If the device also initiates ARP probe with the source address 0.0.0.0, a conflict occurs.
- 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
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.17 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.

 Copyright © Huawei Technologies Co., Ltd.

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 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
```

19.6.18 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.19 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** }

 Copyright © Huawei Technologies Co., Ltd.

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 0 or 30 to 7200, in seconds. The value **0** indicates that the re-authentication function is disabled for users who fail to be authenticated.

Views

Authentication profile 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.

The device cannot re-authenticate wireless users who are in the pre-connection phase or fail authentication. Therefore, the **authentication timer re-authen** command does not apply to wireless 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the authentication profile **authen1**, set the interval for re-authenticating users who fail to be authenticated to 300 seconds.

```
<Huawei> system-view
[Huawei] authentication-profile name authen1
[Huawei-authen-profile-authen1] authentication timer re-authen authen-fail 300
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.20 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

This command applies only to wireless users.

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

In versions earlier than V200R010C00, MAC address authentication is enabled for roaming STAs. 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

 Copyright © Huawei Technologies Co., Ltd.

no longer has the original access permission. To prevent this problem, the MAC address authentication is disabled for roaming STAs by default in V200R010C00 and later versions. 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
```

19.6.21 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	Specifies the interface to allow only one user to go online.	-
single-voice-with-data	Specifies the interface to allow only one data user and one voice user to go online. This mode applies to the scenario in which a data user connects to a network through a voice terminal.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
multi-share	Specifies the interface to allow multiple users to go online. In this mode, the device only authenticates the first user. If the first user can be authenticated, the subsequent users share the same network access rights with the first user. If the first user goes offline, other users are also offline.	-
multi-authen	Specifies the interface to allow multiple users to go online. In this mode, the device authenticates each access user. If users can be authenticated, the users have their individual network access rights. If a user goes offline, other users are not affected. **NOTE** AR100&AR120&AR150&AR160&AR200&AR1200 series do not support to bind a VLAN in MAC-based mode.	-
max-user *max-user-number*	Specifies the maximum number of access users on the interface in **multi-authen** mode.	The value ranges from 1 to 2048 and the default value is 2048.
dot1x	Specifies the maximum number of 802.1X authentication users allowed to connect to the interface in **multi-authen** mode.	-
mac-authen	Specifies the maximum number of MAC address authentication users allowed to connect to the interface in **multi-authen** mode.	-
portal	Specifies the maximum number of Portal authentication 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

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling NAC authentication, you can configure a user access mode based on the user access on the interface. The user access modes include:

- **single-terminal**: applies to the scenario in which only one data terminal is connected to the network through the interface.
- **single-voice-with-data**: applies to the scenario in which only one data terminal is connected to the network on the device interface through a voice terminal.
- **multi-share**: applies to the scenario that does not require high security and in which multiple data terminals are connected to the network on the device interface.
- **multi-authen**: applies to the scenario that requires high security and in which multiple data terminals are connected to the network on the device interface. 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 device interfaces can normally go online.

Precautions

- VLANIF interfaces do not support this function.
- Only wired users support this function.
- If the first access user fails to be authenticated 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 to be authenticated on the interface. Therefore, the following operations are recommended if the first access user may fail to be authenticated after the **multi-share** mode is configured on a physical interface.
  - Do not use the **multi-share** mode with Portal authentication.

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
```

19.6.22 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.23 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.24 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 packets can trigger 802.1X authentication.

 Copyright © Huawei Technologies Co., Ltd.

Format

authentication trigger-condition { **dhcp** | **arp** } *

undo authentication trigger-condition [**dhcp** | **arp**] *

Parameters

Parameter	Description	Value
dhcp	Triggers 802.1X authentication through DHCP packets.	-
arp	Triggers 802.1X authentication through ARP packets.	-

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 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.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

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.

Example

In the 802.1X access profile **d1**, configure the device to use DHCP packets to trigger 802.1X authentication.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] authentication trigger-condition dhcp
```

19.6.25 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 packets can trigger MAC address authentication.

Format

authentication trigger-condition { **dhcp** | **arp** } *

undo authentication trigger-condition [**dhcp** | **arp**] *

Parameters

Parameter	Description	Value
dhcp	Triggers MAC address authentication through DHCP packets.	-
arp	Triggers MAC address authentication through ARP packets.	-

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 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.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- After the VLANIF interface is enabled with the MAC address authentication function, MAC address authentication cannot be triggered for users when the interface receives DHCP packets.
- 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 packets. For wireless users, MAC address authentication is triggered by association 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.

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
```

19.6.26 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.

 Copyright © Huawei Technologies Co., Ltd.

Views

interface or VAP profile

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 **19.6.27 authentication-profile (system view)** command in the system view.

When configuring NAC, pay attention to the following points:

- Layer 2 physical interfaces, Layer 3 physical interfaces, routed main interfaces, VLANIF interfaces, WAN-side interfaces, port groups, and VAP profiles support NAC. The support for authentication types on different interfaces is as follows:
  - Layer 2 physical interfaces: 802.1X authentication, MAC address authentication, and Layer 2 Portal authentication

    NOTE

    The Layer 2 physical interfaces of AR100&AR120&AR150&AR160&AR200 do not support Layer 2 Portal authentication, and support only 802.1X authentication in multicast mode.
  - Layer 3 physical interfaces and routed main interface: Layer 3 Portal authentication

    NOTE

    In wireless scenarios, it does not support Layer 3 Portal authentication.
  - VLANIF interfaces: Layer 2 Portal authentication, MAC address-prioritized Portal authentication in Fat AP Wi-Fi scenarios, and Layer 3 Portal authentication.
  - WAN-side interfaces: Layer 3 Portal authentication
- Physical interfaces do not support multi-mode authentication modes containing Portal authentication.
- 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.
- 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

 Copyright © Huawei Technologies Co., Ltd.

network. In addition, NAC authentication cannot be enabled both on VAP profiles and VLANIF interfaces in wireless scenarios.

- 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.
mac-address learning disable	Disables MAC address learning on an interface.
port-security enable	Enables port security.

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
```

19.6.27 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*

Copyright © Huawei Technologies Co., Ltd.

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 **19.6.26 authentication-profile (Interface view or VAP profile view)** command to apply the authentication profiles to the interface or VAP profile.

Precautions

- The device supports a maximum of 8 authentication profiles. 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 **19.6.31 display**

 Copyright © Huawei Technologies Co., Ltd.

authentication-profile configuration command to check whether the authentication profile is bound to interface or VAP profile

Example

Create the authentication profile named **mac_authen_profile1**.

```
<Huawei> system-view
[Huawei] authentication-profile name mac_authen_profile1
```

Related Topics

19.6.72 dot1x-access-profile (authentication profile view)
19.6.82 mac-access-profile (authentication profile view)
19.6.129 portal-access-profile (authentication profile view)
19.6.31 display authentication-profile configuration

19.6.28 cut web-authentication-user

Function

The **cut web-authentication-user** command configures the device to force Portal authentication users offline when a 3G/LTE link is disconnected.

The **undo cut web-authentication-user** command configures the device not to force Portal authentication users offline when a 3G/LTE link is disconnected.

By default, the Portal authentication users are still online when the 3G/LTE link is disconnected.

Format

cut web-authentication-user [**domain** *domain-name* | **ssid** *ssid*]

undo cut web-authentication-user

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name used in Portal authentication. After this parameter is specified, the device forcibly disconnects the users who use this domain name to go online when the 3G/LTE link is disconnected.	The value must be an existing domain name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ssid *ssid*	Specifies the service set identifier (SSID) of the wireless network. After this parameter is specified, the device forcibly disconnects the users who connect to this wireless network when the 3G/LTE link is disconnected.	The value must be an existing SSID.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

When the router functioning as a mobile Internet gateway is deployed on a bus or metro, only the users who pass Portal authentication can connect to the vehicle-mounted Wi-Fi network and access external networks using the 3G/LTE interface. After the 3G/LTE link is disconnected, the users are not disconnected in real time while they cannot access any web page immediately. This had a negative effect on user experience.

After you run the **cut web-authentication-user** command on the 3G/LTE interface, the device forces Portal authentication users offline when the 3G/LTE link is disconnected. The disconnected users can still access internal network resources of the router, so they can have good user experience.

Example

Configure the device to forcibly disconnect the users who connect to the wireless network **bus-wlan** when the 3G/LTE link is disconnected.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] cut web-authentication-user ssid bus-wlan
```

19.6.29 display access-user

Function

The **display access-user** command displays information about NAC access users.

 Copyright © Huawei Technologies Co., Ltd.

Format

display access-user service-scheme *service-scheme*

display access-user user-group *user-group-name*

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.
user-group *user-group-name*	Displays information about users in a specified user group.	The value must be the name of an existing user group.

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 **huawei**.

```
<Huawei> display access-user service-scheme huawei
--------------------------------------------------------------------------------
UserID Username              IP address      MAC            Status
--------------------------------------------------------------------------------
16018  zqm                   10.12.12.254    78ac-c0c2-0175 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 the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following 19; that is, only 22 characters are displayed.

 Copyright © Huawei Technologies Co., Ltd.

Table 19-40 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.

19.6.30 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

 Copyright © Huawei Technologies Co., Ltd.

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 Eth2/0/0.

```
<Huawei> display authentication interface ethernet 2/0/0
Authentication profile: p1
Port authentication order:
                    MAC
                    DOT1X
                    WEB
```

Table 19-41 Description of the **display authentication interface** command output

Item	Description
Authentication profile	Name of the authentication profile applied to the interface.
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.

19.6.31 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*]

 Copyright © Huawei Technologies Co., Ltd.

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
------------------------------------------------------------------------------
  Total 5, printed 5
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-42 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 aging time                      : 82800s
  Pre-auth aging time                       : 82800s
  Dot1x-mac-bypass                          : Disable
  Single-access                         : Disable
  Device-type authorize service-scheme        : -
  Authentication mode                       : multi-authen
  Authen-fail authorize service-scheme        : -
  Authen-server-down authorize service-scheme : -
  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
  IP-address arp-delay                      : Disable
  Update-session-mode                         : Disable
  Linkdown offline delay time                 : 50
  LDAP-server template                      : -
  AD-server template                        : -
  Termination action                        : reauthenticate
  Authentication roam pre-authen mac-authen   : Enable
```

Table 19-43 Description of the **display authentication-profile configuration name** command output

Item	Description
Profile name	Authentication profile name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dot1x access profile name	802.1X access profile bound to the authentication profile. To configure an 802.1X access profile, run the **19.6.72 dot1x-access-profile (authentication profile view)** command.
Mac access profile name	MAC access profile bound to the authentication profile. To configure a MAC access profile, run the **19.6.82 mac-access-profile (authentication profile view)** command.
Portal access profile name	Portal access profile bound to the authentication profile. To configure a Portal access profile, run the **19.6.129 portal-access-profile (authentication profile view)** command.
Free rule template	Authentication-free rule profile bound to the authentication profile. To configure an authentication-free rule profile, run the **19.6.76 free-rule-template (authentication profile view)** command.
Force domain	Forcible domain for users. To configure a forcible domain, run the **19.6.1 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 **19.6.1 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 **19.6.1 access-domain** command.
Portal force domain	Forcible domain for Portal authentication users. To configure a forcible domain for Portal authentication users, run the **19.6.1 access-domain** command.
Default domain	Default domain for users. To configure a default domain for users, run the **19.6.1 access-domain** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dot1x default domain	Default domain for 802.1X authentication users. To configure a default domain for 802.1X authentication users, run the **19.6.1 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 **19.6.1 access-domain** command.
Portal default domain	Default domain for Portal authentication users. To configure a default domain for Portal authentication users, run the **19.6.1 access-domain** command.
Permit domain	Permitted domain for users. To configure a permitted domain, run the **19.1.74 permit-domain** command.
Authentication handshake	Whether the handshake function is enabled. • Enable • Disable To enable the handshake function, run the **19.6.6 authentication handshake** command.
Authentication handshake period	Handshake interval. To configure the handshake interval, run the **19.6.16 authentication timer handshake-period** command.
Auth-fail re-auth period	Interval for re-authenticating users who fail to be authenticated. To configure the interval, run the **19.6.19 authentication timer re-authen** command.
Pre-auth re-auth period	Interval for re-authenticating pre-connection users. To configure the interval, run the **19.6.19 authentication timer re-authen** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Auth-fail aging Time	Aging time for entries of the users who fail to be authenticated. To configure the aging time, run the **19.6.17 authentication timer authen-fail-aging** command.
Pre-auth aging Time	Aging time for pre-connection user entries. To configure the aging time, run the **19.6.18 authentication timer pre-authen-aging** command.
Dot1x-mac-bypass	Whether MAC address bypass authentication is enabled. • Enable • Disable To configure the function, run the **19.6.8 authentication dot1x-mac-bypass** command.
Single-access	Whether the device allows users to access in only one authentication mode. To configure the function, run the **19.6.15 authentication single-access** command.
Authentication mode	User access mode. To configure the mode, run the **19.6.21 authentication mode** command.
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 **19.6.9 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 **19.6.9 authentication event action authorize** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **19.6.9 authentication event action authorize** command.
Security-name-delimiter	Security string delimiter. To configure the delimiter, run the **19.1.88 security-name-delimiter** command.
Domain-name-delimiter	Domain name delimiter. To configure the delimiter, run the **19.1.53 domain-name-delimiter** command.
Domain-location	Domain name location. To configure the location, run the **19.1.52 domain-location** command.
Domainname-parse-direction	Domain name resolution direction. To configure the direction, run the **19.1.54 domainname-parse-direction** command.
Bound vap profile	VAP profile to which the authentication profile is bound. To configure the VAP profile, run the **19.6.26 authentication-profile (Interface view or VAP profile view)** command.
SVF flag	The flag of SVF status. • Enable • Disable
Ip-static-user	Whether the function of identifying static users through IP addresses is enabled. • Enable • Disable
Roam-realtime-accounting	Whether a device is enabled to send accounting packets for roaming. • Enable • Disable To configure the function, run the **19.1.17 authentication { roam-accounting | update-ip-accounting } * enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Update-IP-realtime-accounting	Whether a device is enabled to send accounting packets for address updating. • Enable • Disable To configure the function, run the **19.1.17 authentication { roam-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 **19.6.81 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 **19.6.14 authentication ip-address in-accounting-start** command.
Update-session-mode	Whether to use the accounting session update mode during roaming accounting. • Enable • Disable To configure the function, run the **19.1.18 authentication roam-accounting update-session-mode**.
LDAP-server template	LDAP server template bound to the authentication profile.
AD-server template	AD server template bound to the authentication profile.
Termination action	Action that the device takes when the timeout period specified by the Session-Timeout attribute delivered by the RADIUS server expires. • reauthenticate To configure the function, run the **19.6.23 authentication termination-action reauthenticate** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication roam pre-authen mac-authen	Whether to enable MAC address authentication for roaming STAs. • Enable • Disable To configure this function, run the **19.6.20 authentication roam pre-authen mac-authen enable** command.

19.6.32 display dot1x

Function

The **display dot1x** command displays 802.1X authentication information.

Format

display dot1x [**statistics**] [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-5>]

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-number* specifies the interface number. If this parameter is not specified, 802.1X authentication information of all interfaces is displayed.	-

Copyright © Huawei Technologies Co., Ltd.

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.

Display 802.1X statistics.

```
<Huawei> display dot1x statistics
  Max users: 2048
  Current users: 0
  Global default domain is default
  Quiet function is Disabled
  Mc-trigger port-up-send is Enabled
  Parameter set:Quiet Period                60s   Quiet-times         3
                Tx Period                   30s   Mac-By-Pass Delay   30s
  Dot1x URL: Not configed.

 GigabitEthernet7/0/0 status: DOWN  802.1x protocol is
Enabled
  Controlled User(s) amount to  0

  Authentication Success: 0          Failure: 0
  Enter Enquence        : 0
  EAPOL Packets: TX     : 1          RX     : 0
  Sent      EAPOL Request/Identity Packets       : 0
            EAPOL Request/Challenge Packets      : 0
            Multicast Trigger Packets            : 1
            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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-44 Description of the **display dot1x** command output

Item	Description
Max users	Maximum number of global online users.
Current users	Number of current online users.
Global default domain is	Global default authentication domain. To configure the global default authentication domain, run the **19.1.51 domain (system view)** command.
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.
Dot1x access profile is	802.1X access profile name. To configure the 802.1X access profile name, run the **19.6.73 dot1x-access-profile (system view)** command.
Authentication mode is	User access mode. To configure the user access mode, run the **19.6.21 authentication mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication method is	Authentication mode of 802.1X users. To configure the authentication mode of 802.1X users, run the **19.6.55 dot1x authentication-method** command.
Reauthentication is	Whether re-authentication is enabled for online 802.1X users. To configure the function, run the **19.6.63 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 **19.6.64 dot1x retry** command.
Authenticating users	Number of users who are being authenticated.
Maximum users	Maximum number of online users on the interface.
Current users	Number of online users on the interface.
Authentication Success Failure	Number of successful and 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: TX RX	Number of globally received and sent EAPOL packets.
EAPOL Request/ Identity Packets	Number of globally received and sent EAPOL Request/ Identity packets.
EAPOL Request/ Challenge Packets	Number of globally received and sent EAPOL Request/ Challenge packets.
Multicast Trigger Packets	Number of globally received and sent multicast packets that trigger authentication.
EAPOL Success Packets	Number of globally received and sent EAPOL Success packets.
EAPOL Failure Packets	Number of globally received and sent EAPOL Failure packets.
EAPOL Start Packets	Number of globally received and sent EAPOL Start packets.
EAPOL Logoff Packets	Number of globally received and sent EAPOL LogOff packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
EAPOL Response/ Identity Packets	Number of globally received and sent EAPOL Response/ Identity packets.
EAPOL Response/ Challenge Packets	Number of globally received and sent EAPOL Response/ Challenge packets.
Controlled User(s) amount to	Number of users who pass authentication successfully.

19.6.33 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

 Copyright © Huawei Technologies Co., Ltd.

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 19-45 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                   : Disable
  Client-no-response authorize : -
  Trigger condition           :
  Unicast trigger             : Disable
  Trigger dhcp-bind       : Disable
  Handshake                   : Disable
  Max retry value             : 2
  Reauthen Period             : 3600s
  Client Timeout              : 5s
  Handshake Period            : 15s
  Bound authentication profile : p2
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-46 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 **19.6.55 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 **19.6.74 dot1x port-control** command.
Re-authen	Whether re-authentication for online 802.1X users is enabled: • Enable • Disable To configure the re-authentication function, run the **19.6.63 dot1x reauthenticate** command.
Client-no-response authorize	Network access rights granted to users when the 802.1X client does not respond. To configure the network access rights, run the **19.6.11 authentication event client-no-response action authorize** command.
Trigger condition	Packet type that can trigger 802.1X authentication: • dhcp • arp To configure the packet type, run the **19.6.24 authentication trigger-condition (802.1X authentication)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Unicast trigger	Whether 802.1X authentication triggered by unicast packets is enabled: • Enable • Disable To configure the function, run the **19.6.70 dot1x unicast-trigger** command.
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 **19.6.67 dot1x trigger dhcp-binding** command.
Handshake	Whether handshake with online 802.1X authentication users is enabled: • Enable • Disable To configure the function, run the **19.6.57 dot1x handshake** command.
Max retry value	Maximum number of attempts to send authentication requests to 802.1X users. To configure the maximum value, run the **19.6.64 dot1x retry** command.
Reauthen Period	Re-authentication interval for online 802.1X users. To configure the re-authentication interval, run the **19.6.65 dot1x timer** command.
Client Timeout	Authentication timeout period for 802.1X clients. To configure the authentication timeout period, run the **19.6.65 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 **19.6.65 dot1x timer** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Bound authentication profile	Authentication profile to which the 802.1X access profile is bound. To configure the authentication profile, run the **19.6.72 dot1x-access-profile (authentication profile view)** command.

19.6.34 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display dot1x quiet-user all
--------------------------------------------------------------------------------
MacAddress                                Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
0001-0002-0003                            50
--------------------------------------------------------------------------------
1 silent mac address(es) found, 1 printed.
```

Table 19-47 Description of the **display dot1x quiet-user all** command output

Item	Description
MacAddress	MAC address of an 802.1X authentication user who is quieted.
Quiet Remain Time(Sec)	Remaining quiet time of an 802.1X authentication user who is quieted, in seconds.

19.6.35 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.

 Copyright © Huawei Technologies Co., Ltd.

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 19-48 Description of the **display free-rule-template configuration** command output

Item	Description
ID	ID of an authentication-free rule profile.
Free-rule-template Name	Name of an authentication-free rule profile.

19.6.36 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*]

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.	-

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/Bridge/VSI     Learned-From          Type
-------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
0000-0000-0100    3000                GE2/0/0         authen
0000-0000-0400    3000                GE2/0/0         authen
0000-0000-0200    3000                GE2/0/0         authen
--------------------------------------------------------------------------------
Total items displayed = 3
```

Table 19-49 Description of the **display mac-address authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/Bridge/VSI	VLAN/Bridge/VSI 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.

19.6.37 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*]

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.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

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/Bridge/VSI       Learned-From            Type
--------------------------------------------------------------------------------
0000-0000-0100    3000                      GE2/0/0         pre-authen
0000-0000-0400    3000                      GE2/0/0         pre-authen
0000-0000-0200    3000                      GE2/0/0         pre-authen
--------------------------------------------------------------------------------
Total items displayed = 3
```

Table 19-50 Description of the **display mac-address pre-authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/Bridge/VSI	VLAN/Bridge/VSI 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.

 Copyright © Huawei Technologies Co., Ltd.

19.6.38 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.

 Copyright © Huawei Technologies Co., Ltd.

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 19-51 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
  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
  Trigger dhcp-bind          : Enable
  Reauthen Period            : 1800s
  Bound authentication profile : -
```

Table 19-52 Description of the **display mac-access-profile configuration name** command output

Item	Description
Profile Name	MAC access profile name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication method	Authentication mode for MAC address authentication. • CHAP • PAP To configure the authentication mode, run the **19.6.84 mac-authen authentication-method** command.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.93 mac-authen username** command.
Password type	Password display mode for MAC address authentication. • cipher To configure the password display mode, run the **19.6.93 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 **19.6.89 mac-authen reauthenticate** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trigger condition	Packet type that can trigger MAC address authentication. To configure the packet type, run the **19.6.25 authentication trigger-condition (MAC address authentication)** 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 **19.6.92 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 **19.6.91 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 **19.6.82 mac-access-profile (authentication profile view)** command.

19.6.39 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*] } &<1-5> | **configuration**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays MAC authentication information of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display mac-authen
  Quiet period is 60s
  Authentication fail times before quiet is 1
  Maximum users: 2048
  Current users: 1
  Global default domain is default

GigabitEthernet2/0/0 state: UP.  MAC address authentication is enabled
  MAC access profile is mac_access_profile
  Reauthentication is disabled
  Maximum users: 2048
  Current users: 1
  Username format: fixed username: gcs
  Password type: cipher
  Fixed password: %^%#2}*{%bMY.D*Kw3HxDgU3CW7g'|54H&<]S,Zfu;%^%#
  Authentication Success: 22, Failure: 85

Online user(s) info:
UserId   MAC/VLAN          AccessTime            UserName
------------------------------------------------------------------------------
37223    a088-b44d-573c/2003 2014/09/28 15:45:45    gcs
------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 19-53 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 **19.6.90 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 **19.6.87 mac-authen quiet-times** command.
Maximum users	Maximum number of users allowed on the device.
Current users	Number of online users.
Global default domain	Global default authentication domain. To configure the global default authentication domain, run the **19.1.51 domain (system view)** command.
interface state	Interface status: • UP: The interface is enabled. • DOWN: The interface is shut down.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **19.6.83 mac-access-profile (system view)** command.
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 **19.6.89 mac-authen reauthenticate** command.
Current users	Number of current online users on the interface.

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	contains colons (:) and the colons are inserted between every two digits, for example, 00:05:e0:1c:02:e3. • 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 for MAC address authentication, run the **19.6.93 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 **19.6.93 mac-authen username** command.
Fixed password	Password for MAC address authentication. To configure the password for MAC address authentication, run the **19.6.93 mac-authen username** command.
Authentication Success: *m*, Failure: *n*	Numbers of successful authentications (*m*) and failed authentications (*n*) on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Online user(s) info	Online user information. • 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.

19.6.40 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

 Copyright © Huawei Technologies Co., Ltd.

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                                Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
0001-0002-0003                             50
--------------------------------------------------------------------------------
1 silent mac address(es) found, 1 printed.
```

Table 19-54 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.
Quiet Remain Time(Sec)	Remaining quiet time of a MAC address authentication user who is quieted, in seconds.

19.6.41 display portal

Function

The **display portal** command displays the Portal authentication configuration.

Format

display portal [**interface** *interface-type interface-number* | **configuration**]

 Copyright © Huawei Technologies Co., Ltd.

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:2048
  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

  Vlanif10 protocol status: down, web-auth-server layer2(direct)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-55 Description of the **display portal** command output

Item	Description
Portal max-user number	Maximum number of concurrent Portal authentication users allowed to access the device. To set the maximum number of concurrent Portal authentication users allowed to access the device, run the **19.6.120 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 **19.6.121 portal quiet-period** command.
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 **19.6.118 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 **19.6.123 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 **19.6.122 portal quiet-times** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **19.6.119 portal logout resend timeout** command.
Portal Https Redirect	Whether HTTPS redirection of Portal authentication is enabled: • Enable • Disable To enable this function, run the **19.6.102 portal https-redirect enable** command.
interface protocol status	Link layer protocol state of the interface. • 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.

19.6.42 display portal local-server connect

Function

The **display portal local-server connect** command displays the connection status of users to be authenticated on a built-in Portal server.

Format

display portal local-server connect [**user-ip** *ip-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
user-ip *ip-address*	Displays the connection entry of a user with a specified IP address on a built-in Portal server. The connection entries of all users on the built-in Portal server are displayed if this parameter is not specified.	The value of *ip-address* is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display portal local-server connect** command to check the authentication mode and status of users to be authenticated on a built-in Portal server.

Example

Display the connection status of the user with the IP address 10.1.1.10 on a built-in Portal server.

```
<Huawei> display portal local-server connect user-ip 10.1.1.10
------------------------------------------------------------------------------
 CID  IP Address   AuthMode  State    Session-timeout(hours)
------------------------------------------------------------------------------
 1    10.1.1.10    CHAP      ONLINE   8
------------------------------------------------------------------------------
```

Table 19-56 Description of the **display portal local-server connect** command output

Item	Description
CID	User table index.
IP Address	IP address of a user.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AuthMode	Authentication mode: • CHAP: The built-in Portal server uses CHAP to authenticate the user. • PAP: The built-in Portal server uses PAP to authenticate the user. To set the authentication method, run the **19.6.104 portal local-server authentication-method** command.
State	User status: • WAIT_CHALLENGE: waiting for the challenge • WAIT_AUTHACK: waiting for the authentication response • ONLINE: online • WAIT_LOGOUTACK: waiting for logout
Session-timeout(hours)	The session timeout interval. To set the session timeout interval, run the **19.6.117 portal local-server timer session-timeout**.

19.6.43 display portal local-server

Function

The **display portal local-server** command displays the configurations of a built-in Portal server.

Format

display portal local-server

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After configuring the built-in Portal authentication, run this command to view the configurations of a built-in Portal server.

Example

Display the configurations of a built-in Portal server.

```
<Huawei> display portal local-server
 Portal local-server config:
  server status                : disable
  Heartbeat-check status       : auto
  Heartbeat-timeout value      : 60(s)
  server ip                    : 10.1.1.1
  authentication method        : chap
  protocol                     : -
  https ssl-policy             : -
  server port                  : 0
  session-timeout              : 8(h)
  syslog-limit                 : enable
  syslog-limit period          : 300(s)
  server pagename              : -
  server page-text             : -
  server policy-text           : -
  server background-image      : default-image0
  server background-color      : -
  server logo                  : -
  server ad-image              : -
```

Table 19-57 Description of the **display portal local-server** command output

Item	Description
server status	Status of a built-in Portal server. To enable the built-in Portal server function, run the **portal local-server** command. • disable: Portal authentication is disabled. • enable: Portal authentication is enabled.
Heartbeat-check status	Heartbeat detection status of the built-in Portal server. To set the heartbeat detection status, run the **19.6.109 portal local-server keep-alive** command. • disable: indicates that the heartbeat detection function is disabled. • enable: indicates the forcible detection mode. • auto: indicates the automatic detection mode.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Heartbeat-timeout value	Heartbeat detection interval of the built-in Portal server. To set the heartbeat detection interval, run the **19.6.109 portal local-server keep-alive** command. This parameter is unavailable when the value of **Heartbeat-check status** is **disable**.
server ip	IP address of a built-in Portal server. To set the server IP address, run the **portal local-server ip** command.
authentication method	Authentication method used by a built-in Portal server for web users. To set the authentication method, run the **portal local-server authentication-method** command. • chap: CHAP-based authentication (CHAP stands for Challenge Handshake Authentication Protocol.) • pap: PAP-based authentication (PAP stands for Password Authentication Protocol.)
protocol	Protocol used for authentication information exchange between a built-in Portal server and users. To enable the built-in Portal server function, run the **portal local-server** command.
https ssl-policy	SSL policy used for authentication information exchange between a built-in Portal server and users. To enable the built-in Portal server function, run the **portal local-server** command.
server port	TCP port number used by HTTPS. To specify a TCP port number used by HTTPS, run the **portal local-server** command.
session-timeout	User session timeout interval configured on the built-in Portal server. To set the session timeout interval, run the **portal local-server timer session-timeout** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
syslog-limit	Status of the log suppression function for built-in Portal authentication users. To enable or disable the log suppression function, run the **19.6.115 portal local-server syslog-limit enable** command. • disable: indicates that the log suppression function is disabled for built-in Portal authentication users. • enable: indicates that the log suppression function is enabled for built-in Portal authentication users.
syslog-limit period	Log suppression duration for built-in Portal authentication users. To set the log suppression duration, run the **19.6.116 portal local-server syslog-limit period** command.
server pagename	Name of the page file package loaded to the built-in Portal server. To set the package name, run the **19.6.110 portal local-server load** command.
server page-text	Loaded use instruction page file of the built-in Portal server. To load a use instruction page file, run the **19.6.113 portal local-server page-text load** command.
server policy-text	Disclaimer page loaded to the built-in Portal server. To load a disclaimer page, run the **19.6.114 portal local-server policy-text load** command.
server background-image	Background image of the built-in Portal server login page. To set the background image, run the **19.6.106 portal local-server background-image load** command.
server background-color	Background color of the built-in Portal server login page. To set the background color, run the **19.6.105 portal local-server background-color** command.
server logo	Logo file of the built-in Portal server login page. To load a logo file, run the **19.6.111 portal local-server logo load** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
server ad-image	Advertisement image file of the built-in Portal server login page. To load an advertisement image file, run the **19.6.103 portal local-server ad-image load** command.

19.6.44 display portal local-server page-information

Function

The **display portal local-server page-information** command displays the page files loaded to the memory of a built-in Portal server.

Format

display portal local-server page-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display portal local-server page-information** command to check the page files loaded to the memory of a built-in Portal server.

Example

Display the page files loaded to the memory of a built-in Portal server.

```
<Huawei> display portal local-server page-information
------------------------------------------------------------------------------
    Number of backup pages:35
    Size of backup pages:94438 byte
------------------------------------------------------------------------------
    Name:/logout_success.html
    Size:4042 byte
    Last-Modified-Time:2011-12-16 20:24:46
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-58 Description of the **display portal local-server page-information** command output

Item	Description
Number of backup pages	Number of page files loaded.
Size of backup pages	Total size of the loaded page files.
Name	Name of a page file.
Size	Size of a page file.
Last-Modified-Time	Last modification time.

Related Topics

19.6.110 portal local-server load

19.6.45 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.

Copyright © Huawei Technologies Co., Ltd.

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 19-59 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
  User-group name                 : -
  Re-auth                         : Disable
  Network IP Num                  : 3
  Network IP List                 : 10.1.1.0 255.255.255.0
                                    10.10.1.0 255.255.255.0
                                    10.1.2.0 255.255.255.0
  Web-auth-server Name            : s1
  Layer                           : Layer two portal
  Local-server                    : Disable
  Bound authentication profile    : -
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-60 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 **19.6.124 portal timer offline-detect** command.
User-group name	Name of the user group based on which the device assigns network access rights to users when the Portal server is Down. To configure the user group name, run the **19.6.12 authentication event portal-server-down action authorize** command.
Re-auth	Whether the device is enabled to re-authenticate users when the Portal server changes from Down to Up. To configure the function, run the **19.6.13 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 **19.6.99 portal auth-network** command.
Network IP List	Source IP address segment for Portal authentication. To configure the source IP address segment, run the **19.6.99 portal auth-network** command.
Web-auth-server Name	Portal server profile bound to the Portal access profile. To configure the Portal server profile, run the **19.6.155 web-auth-server (Portal access profile view)** command.
Layer	Portal authentication mode. To configure the Portal authentication mode, run the **19.6.155 web-auth-server (Portal access profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Local-server	Whether the built-in Portal server function is enabled. To configure the built-in Portal server function, run the **19.6.107 portal local-server enable** command.
Bound authentication profile	Authentication profile to which the portal access profile is bound. To configure the authentication profile, run the **19.6.129 portal-access-profile (authentication profile view)** command.

19.6.46 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

 Copyright © Huawei Technologies Co., Ltd.

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                                    Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
192.168.1.1                                 10
192.168.1.2                                 20
--------------------------------------------------------------------------------
2 quiet IP found, 2 printed.
```

Display information about all the users in quiet state authenticated by the Portal authentication server with IP address 192.168.2.1.

```
<Huawei> display portal quiet-user server-ip 192.168.2.1
Quiet IP information
--------------------------------------------------------------------------------
Quiet ip                                    Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
192.168.1.3                                 10
192.168.1.4                                 20
--------------------------------------------------------------------------------
2 quiet IP found, 2 printed.
```

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 second     100
```

Table 19-61 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.
Quiet Remain Time(Sec)	Remaining quiet time of the user in quiet state, in seconds.
Quiet remain second	Remaining quiet period of the user in quiet state.

19.6.47 display portal url-encode configuration

Function

The **display portal url-encode configuration** command displays the configuration of URL encoding and decoding.

 Copyright © Huawei Technologies Co., Ltd.

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 19-62 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 **19.6.128 portal url-encode enable** command.

Related Topics

19.6.128 portal url-encode enable

19.6.48 display portal user-logout

Function

The **display portal user-logout** command displays temporary logout entries of Portal authentication users.

Copyright © Huawei Technologies Co., Ltd.

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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-63 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 **19.6.119 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.

19.6.49 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 profile. If this parameter is not specified, status of all Portal servers is displayed.	The Portal server profile name must exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When an external Portal server is used for Portal authentication, you 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 profile **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 19-64 Description of the **display server-detect state** command output

Item	Description
Web-auth-server	Name of the Portal server profile.
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 profile view.
Status	Status of the Portal server. The values are as follows: • Normal: indicates that the Portal server is in normal state. When *Total-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 *Total-servers* in the command output is less than or equal to *Critical-num*, *Status* is displayed as **Abnormal**.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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

Related Topics

19.6.136 server-ip (Portal server profile view)
19.6.135 server-detect

19.6.50 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, run the **display url-template** command to view information about the URL template.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about all configured URL templates.

```
<Huawei> display url-template all

-------------------------------------------------------------------------------
 Name                        URL     Start  Assignment  Isolate
                           Number  Mark   Mark        Mark
-------------------------------------------------------------------------------
 huawei                       0      ?     =           &
 huawei2                      0      ?     =           &
 huawei3                      0      ?     =           &
-------------------------------------------------------------------------------
 Total 3
```

Display information about the URL template **huawei**.

```
<Huawei> display url-template name huawei
 Name : huawei
 URL  :
 Start mark      : ?
 Assignment mark : =
 Isolate mark    : &
 AC IP           :
 AC MAC          :
 AP IP           :
 AP MAC          :
 SSID            :
 User MAC        :
 Redirect URL    :
 User IP address :
 Sysname         :
 User VLAN       :
 Delimiter       :
 Format          :
 Ac-ip Value     : 10.1.1.1
 Ap-ip Value     : Vlanif10
 ESN             :
```

Table 19-65 Description of the **display url-template** command output

Item	Description
Name	Name of a URL template.
URL Number	Number of URLs.
URL	URL of the Portal server. To configure this parameter, run the **19.6.142 url (URL template view)** command.
Start mark/Start Mark	Start character in the URL. To configure this parameter, run the **19.6.97 parameter** command.
Assignment mark/Assignment Mark	Assignment character in the URL. To configure this parameter, run the **19.6.97 parameter** command.
Isolate mark/Isolate Mark	Delimiter between URLs. To configure this parameter, run the **19.6.97 parameter** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AC IP	Name of **ac-ip** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
AC MAC	Name of **ac-mac** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
AP IP	Name of **ap-ip** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
AP MAC	Name of **ap-mac** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
SSID	Name of **ssid** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
User MAC	Name of **user-mac** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
Redirect URL	Name of **redirect-url** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
User IP address	Name of **user-mac** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
Sysname	Name of **sysname** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
User VLAN	Name of **user-vlan** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
Delimiter	Delimiter between MAC addresses in the URL. To configure this parameter, run the **19.6.144 url-parameter mac-address format** command.
Format	Format of MAC addresses in the URL. To configure this parameter, run the **19.6.144 url-parameter mac-address format** command.
ESN	Name of **esn** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ac-ip Value	Value of the redirection parameter **ac-ip**. To configure this parameter, run the **19.6.146 url-parameter set** command.
Ap-ip Value	Value of the redirection parameter **ap-ip**. To configure this parameter, run the **19.6.146 url-parameter set** command.

19.6.51 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 user group with a specified name. If this parameter is not specified, the configurations of all user groups are displayed.	The value must be the name of an existing user group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a user group, you can run this command to check whether the configuration is correct.

Example

Display the configurations of all user groups.

```
<Huawei> display user-group
--------------------------------------------------------------------------------
ID   Group name                      User-num
```

 Copyright © Huawei Technologies Co., Ltd.

```
--------------------------------------------------------------------------------
0     g1                            0
--------------------------------------------------------------------------------
Total 1
```

NOTE

When the length of **Group name** exceeds 14 characters, the name is displayed in abridged mode.

Display the configuration of the user group **g1**.

```
<Huawei> display user-group g1
  User group ID          : 0
  Group name             : g1
  ACL ID                 :
  ACL rule number        : 0
  User-num               : 0
  VLAN                   :
  Remark dscp            :
  Remark 8021p           :
  Remark exp             :
  Remark lp              :
  IsolateInter           : No
  IsolateInner           : No
```

Table 19-66 Description of the **display user-group** command output

Item	Description
ID/User group ID	User group ID.
Group name	User group name.
ACL ID	ID of the IPv4 ACL bound to the user group. To configure the ACL ID, run the **19.6.5 acl-id (user group view)** command.
ACL rule number	Number of ACL rules.
User-num	Number of online users bound to the user group.
VLAN	VLAN bound to the user group. To configure the VLAN, run the **19.6.152 user-vlan** command.
Remark dscp	Priorities for processing IP packets. To set the priorities, run the **19.6.132 remark** command.
Remark 8021p	Priorities for processing Ethernet Layer 2 packets. To set the priorities, run the **19.6.132 remark** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remark exp	Processing priority of MPLS packets. To set the priorities, run the **19.6.132 remark** command.
Remark lp	Processing priority of internal packets. To set the priorities, run the **19.6.132 remark** command.
IsolateInter	Inter-group user isolation.
IsolateInner	Intra-group user isolation.

19.6.52 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

------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
Web-auth-server Name : huawei
IP-address           :
Shared-key           :
Source-IP            : -
Port / PortFlag      : 50100 / NO
URL                  : https://192.168.2.10:8443/webauth
URL Template         :
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        :
VPN Instance         :
Bound Portal profile :

Protocol             : portal


------------------------------------------------------------------------------
1 Web authentication server(s) in total
```

Table 19-67 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 **19.6.154 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 **19.6.158 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 **19.6.156 web-auth-server reply-message** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Web-auth-server Name	Name of the Portal server template. To configure the Portal server template name, run the **19.6.157 web-auth-server (system view)** command.
IP-address	IP address of the Portal server. To configure the IP address of the Portal server, run the **19.6.136 server-ip (Portal server profile view)** command.
Shared-key	Shared key of the Portal server. To configure the shared key of the Portal server, run the **19.6.137 shared-key (Portal server profile view)** 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 **19.6.139 source-ip (Portal server profile view)** 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 **19.6.98 port (Portal server profile view)** command.
URL	URL of the Portal server. To configure the URL of the Portal server, run the **19.6.143 url (Portal server profile view)** command.
URL Template	URL template bound to the Portal server template. To configure the URL template, run the **19.6.148 url-template (Portal server profile view)** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **19.6.159 web-redirection disable (Portal server profile view)** command.
Sync	User information synchronization. To enable user information synchronization, run the **19.6.149 user-sync** command.
Sync Seconds	User information synchronization interval. To set the user information synchronization interval, run the **19.6.149 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 **19.6.149 user-sync** command.
Detect	Portal server detection function. To configure Portal server detection function, run the **19.6.135 server-detect** command.
Detect Seconds	Detection interval of the Portal server. To set the detection interval of the Portal server, run the **19.6.135 server-detect** command.
Detect Max-times	Maximum number of detection failures. To set the maximum number of detection failures, run the **19.6.135 server-detect** command.
Detect Critical-num	Minimum number of Portal servers in Up state. To configure this function, run the **19.6.135 server-detect** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **19.6.135 server-detect** command.
VPN Instance	VPN instance used in Portal authentication. To configure the VPN instance, run the **19.6.153 vpn-instance (Portal server template view)** command.
Bound Portal profile	Portal access profile to which the Portal server template is bound. To configure the Portal access profile, run the **19.6.155 web-auth-server (Portal access profile view)** command.
Protocol	Protocol used in Portal authentication. • Portal • haca To configure the protocol, run the **19.6.127 protocol** command.

19.6.53 display snmp-agent trap feature-name mid_eapol all

Function

The **display snmp-agent trap feature-name mid_eapol all** command displays the status of all traps on the DOT1X module.

Format

display snmp-agent trap feature-name mid_eapol all

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the DOT1X module, you can run this command to check the status of all traps on the DOT1X module. To enable the trap function for the DOT1X module, run the **snmp-agent trap enable feature-name mid_eapol** command.

Prerequisites

The SNMP function has been enabled on the device. For details, see **snmp-agent**.

Example

Display the status of all traps on the DOT1X module.

```
<Huawei> display snmp-agent trap feature-name mid_eapol all
------------------------------------------------------------------------------
Feature name: MID_EAPOL
Trap number : 2
------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwSrvcfgEapMaxUserAlarm      on                      on
hwMacAuthenMaxUserAlarm      on                      on
```

Table 19-68 Description of the **display snmp-agent trap feature-name mid_eapol all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.
Trap name	Name of a trap. Traps on the DOT1X module include: • hwSrvcfgEapMaxUserAlarm: The device sends a Huawei proprietary trap when the number of 802.1X authentication users reaches the maximum number allowed on an interface. • hwMacAuthenMaxUserAlarm: The device sends a Huawei proprietary trap when the number of MAC address authentication users reaches the maximum number allowed on an interface.
Default switch status	Default status of the trap function: • on: The trap function is enabled by default. • off: The trap function is disabled by default.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Trap status: • on: The trap is enabled. • off: The trap is disabled.

Related Topics

19.6.140 snmp-agent trap enable feature-name mid_eapol

19.6.54 display snmp-agent trap feature-name mid_web all

Function

The **display snmp-agent trap feature-name mid_web all** command displays the status of all traps on the web authentication module.

Format

display snmp-agent trap feature-name mid_web all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the web authentication module, you can run this command to check the status of all traps on the web authentication module. To enable the trap function for the web authentication module, run the **snmp-agent trap enable feature-name mid_web** command.

Prerequisites

The SNMP function has been enabled on the device. For details, see **snmp-agent**.

Example

Display the status of all traps on the web authentication module.

```
<Huawei> display snmp-agent trap feature-name mid_web all
------------------------------------------------------------------------------
Feature name: MID_WEB
```

 Copyright © Huawei Technologies Co., Ltd.

```
Trap number : 4
------------------------------------------------------------------------------
Trap name                Default switch status   Current switch status
hwPortalServerUp              on                      on
hwPortalServerDown            on                      on
hwPortalMaxUserAlarm          on                      on
hwPortalUserClearAlarm        on                      on
```

Table 19-69 Description of the **display snmp-agent trap feature-name mid_web all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.
Trap name	Name of a trap. Traps on the web authentication module include: • hwPortalServerUp: The device sends a Huawei proprietary trap when it detects that the Portal server changes from Down to Up. • hwPortalServerDown: The device sends a Huawei proprietary trap when it detects that the Portal server changes from Up to Down. • hwPortalMaxUserAlarm: The device sends a Huawei proprietary trap when the number of online Portal authentication users exceeds the upper threshold. • hwPortalUserClearAlarm: The device sends a Huawei proprietary trap when the number of online Portal authentication users falls below the lower threshold.
Default switch status	Default status of the trap function: • on: The trap function is enabled by default. • off: The trap function is disabled by default.
Current switch status	Trap status: • on: The trap is enabled. • off: The trap is disabled.

Related Topics

19.6.141 snmp-agent trap enable feature-name mid_web

19.6.55 dot1x authentication-method

Function

The **dot1x authentication-method** command configures an 802.1X authentication mode.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

  - 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
```

Related Topics

19.6.33 display dot1x-access-profile configuration

 Copyright © Huawei Technologies Co., Ltd.

19.6.56 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.57 dot1x handshake

Function

The **dot1x handshake** command enables the device to send handshake packets to online 802.1X users.

The **undo dot1x handshake** command disables the device from sending handshake packets to online 802.1X users.

By default, the device handshake function is disabled for online 802.1X users.

Format

dot1x handshake

undo dot1x handshake

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check whether an 802.1X user is online in real time, run the **19.6.6 authentication handshake** command to enable the device to send handshake packets to the 802.1X user. If some clients support handshake with online 802.1X users, run the **dot1x handshake** command to enable handshake with online 802.1X users. Then the device sends EAP handshake request packets to the user. If the user sends a response packet within the handshake interval (configured using the **19.6.65 dot1x timer** command), the device considers that the user is online. If the user does not send any response packet within the interval, the device considers that the user is offline.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Currently, most clients do not support this function, for example, the Windows built-in client, AnyConnect client, and iOS built-in client. If a client does not support the handshake function, the device will not receive handshake response packets within the handshake interval and considers that the user is offline. Therefore, you need to disable the device from sending handshake packets to an online 802.1X user when the user's client does not support the handshake function.

After the **dot1x handshake** command is run, the **19.6.6 authentication handshake** command does not take effect.

This function takes effect only for the wired users.

Example

In the 802.1X access profile **d1**, enable the device to send handshake packets to online 802.1X users.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x handshake
```

19.6.58 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.59 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

In an 802.1X authentication scenario, 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 through EAPOL-Start packets sent by the client immediately after the interface goes Up. This configuration shortens the re-authentication time.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The function of triggering 802.1X authentication through multicast packets has been enabled using the **dot1x mc-trigger** command.

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
[Huawei] dot1x mc-trigger port-up-send enable
```

19.6.60 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 **19.6.61 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 **19.6.66 dot1x timer quiet-period** command. When the quiet timer expires, the device re-authenticates the user.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the quiet timer.

```
<Huawei> system-view
[Huawei] dot1x quiet-period
```

19.6.61 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 **19.6.60 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.62 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 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

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.63 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 **19.6.65 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.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

After re-authentication is configured for online 802.1X authentication users, a large number of 802.1X authentication logs are generated.

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
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.64 dot1x retry

Function

The **dot1x retry** command configures the number of times an authentication request or handshake packet 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 or handshake packet 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 or handshake packet is retransmitted to an 802.1X user.	The value is an integer that ranges from 1 to 10.

Views

802.1X access profile view

 Copyright © Huawei Technologies Co., Ltd.

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 or handshake packet to the user, the device sends the authentication request or handshake packet again. If the authentication request or handshake packet has been sent for the maximum retransmission times and no response is received, the user authentication or handshake fails. In this process, the total number of authentication requests or handshake packets 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*	**19.6.69 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)	**19.6.68 dot1x timer mac-bypass-delay** *delay-time-value*
EAP-Request/MD5 Challenge packet	*client-timeout-value*	**19.6.65 dot1x timer client-timeout** *client-timeout-value*
Handshake packet	*handshake-period-value*	**19.6.65 dot1x timer handshake-period** *handshake-period-value*

Example

In the 802.1X access profile **d1**, configure the number of times an authentication request or handshake packet 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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.65 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* | **handshake-period** *handshake-period-value* }

undo dot1x timer { **client-timeout** | **reauthenticate-period** | **handshake-period** }

Parameters

Parameter	Description	Value
client-timeout *client-timeout-value*	Specifies the client authentication timeout interval. **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 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 60 to 7200, in seconds. By default, the periodic re-authentication period is 3600 seconds for online 802.1X users.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
handshake-period *handshake-period-value*	Specifies the interval at which the device handshakes with an 802.1X client on a non-Eth-Trunk interface. For details, see **19.6.57 dot1x handshake**.	The value is an integer that ranges from 5 to 7200, in seconds. By default, the interval for sending handshake packets is 15s.

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 **19.6.64 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 **19.6.63 dot1x reauthenticate** command.
- The online 802.1X user handshake function is disabled by default. You can run the **19.6.57 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.66 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 **19.6.60 dot1x quiet-period** command, if the number of times that an 802.1X user fails to be authenticated

Copyright © Huawei Technologies Co., Ltd.

within 60s exceeds the upper limit (configured using the **19.6.61 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
```

19.6.67 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

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

 Copyright © Huawei Technologies Co., Ltd.

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.

For detailed configurations of IPSG and DAI, see **IPSG Configuration** and **ARP Security Configuration** in the *Huawei AR Series V200R010 Configuration Guide - Security*.

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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.68 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.64 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
```

19.6.69 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.68 dot1x timer mac-bypass-delay** command and *max-retry-value* configured in the **19.6.64 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
```

19.6.70 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

dot1x unicast-trigger

undo dot1x unicast-trigger

Parameters

None

Views

802.1X access profile view

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.65 dot1x timer client-timeout** *client-timeout-value* command), the device retransmits the unicast packet (the maximum of retransmission times is set by the **19.6.64 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.

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
```

19.6.71 dot1x url

Function

The **dot1x url** command configures the redirect-to URL in 802.1X authentication.

The **undo dot1x url** command cancels the redirect-to URL configuration in 802.1X authentication.

By default, no redirect-to URL is configured in 802.1X authentication.

Format

dot1x url *url-string*

undo dot1x url

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url-string	Specifies the redirect-to URL.	It is a string of 1 to 200 case-sensitive characters that do not contain spaces and question marks (?). 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

In the early stage of network deployment, 802.1X client deployment is difficult with heavy workload. You can run the **dot1x url** command to set the redirect-to URL to the 802.1X client download web page address. When a user attempts to access a non-free IP subnet, the device redirects the user to the redirect-to URL where the user can download and install the 802.1X client software.

Follow-up Procedure

Run the **19.6.75 free-rule** command to configure a free IP subnet where the redirect URL used in 802.1X authentication belongs.

Precautions

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-to URL in 802.1X authentication to http://www.***.com.cn.

```
<Huawei> system-view
[Huawei] dot1x url http://www.***.com.cn
```

19.6.72 dot1x-access-profile (authentication profile view)

Function

The **dot1x-access-profile** command binds an authentication profile to an 802.1X access profile.

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.73 dot1x-access-profile (system view)** command.

Follow-up Procedure

Run the **19.6.26 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**.

 Copyright © Huawei Technologies Co., Ltd.

```
<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
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.73 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

 Copyright © Huawei Technologies Co., Ltd.

VAP profile, bind the authentication profile applied to the interface or VAP profile to an 802.1X access profile.

Follow-up Procedure

Run the **19.6.72 dot1x-access-profile (authentication profile view)** command in the authentication profile view to bind the authentication profile to an 802.1X access profile.

Precautions

- The device supports a maximum of 8 configurable 802.1X access profiles. 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.

Example

Create the 802.1X access profile named **dot1x_access_profile1**.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name dot1x_access_profile1
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.74 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

 Copyright © Huawei Technologies Co., Ltd.

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 EAPOL 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 EAPOL packets, and allows users to access network resources without authentication or authorization. Indicates the forcible unauthorized mode. In this mode, the interface is always in Unauthorized state, does not handle EAPOL packets, and prohibits users from accessing network resources.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
unauthorized-force	Indicates the forcible authorization mode. In this mode, the interface is always in Authorized state, does not handle EAPOL packets, and allows users to access network resources without authentication or authorization. Indicates the forcible unauthorized mode. In this mode, the interface is always in Unauthorized state, does not handle EAPOL packets, and prohibits users from accessing 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.75 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* } | **any** } } | **source** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } } } *

undo free-rule { *rule-id* | **all** }

Authentication-free rule defined by ACL:

free-rule acl *acl-id*

undo free-rule acl

Parameters

Parameter	Description	Value
rule-id	Specifies the number of an authentication-free rule for NAC authentication users.	The value is an integer that ranges from 0 to 39.
destination	Specifies the destination network resource that NAC authentication users can access without authentication.	-
source	Specifies source information for NAC authentication users without authentication.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
any	Indicates any condition. When **any** is used together with different keywords, the effect of the command is different.	-
ip *ip-address*	Specifies the source or destination IP address depending on the keyword.	The value is in dotted decimal notation.
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.
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.
all	Specifies all rules.	-

Views

Authentication-free rule profile 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 running the **19.6.77 free-rule-template (system view)** command 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.

Precautions

Wireless 802.1X authentication does not support this function.

A common authentication-free rule cannot be configured together with an authentication-free rule defined by ACL.

 Copyright © Huawei Technologies Co., Ltd.

The priority of the ACL rule delivered by the RADIUS server is higher than that of the authentication-free rule configured on the device.

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
```

19.6.76 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.

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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.77 free-rule-template (system view)** command.

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
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.35 display free-rule-template configuration

19.6.77 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.75 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**.

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]
```

Related Topics

19.6.35 display free-rule-template configuration

19.6.78 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.79 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-**

 Copyright © Huawei Technologies Co., Ltd.

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 (=).

 Copyright © Huawei Technologies Co., Ltd.

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 authentication server response message is displayed after a user login failure. • **err-msg msg** *msg*: A specified message is displayed after a user login failure. • **redirect-login-url**: A user is redirected to the login URL after a login failure. This mode is the default mode. • **redirect-url** *redirect-url*: A user is redirected to a specified URL after a login failure. • **append-reply-message** *msgkey*: specifies the identification keyword for the authentication server response message carried in the redirection URL.	• *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 200 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 (=).

 Copyright © Huawei Technologies Co., Ltd.

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 after successful user login. • **redirect-init-url**: A user is redirected to the initial login URL after successful login. This mode is the default mode. • **redirect-url** *redirect-url*: A user is redirected to a specified URL after 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 200 case-sensitive characters without spaces.
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 after a user logout failure. The default value is **LogoutFail!**. • **redirect-url** *redirect-url*: A user is redirected to a specified URL after 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 200 case-sensitive characters without spaces.
logout-success response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon successful user logout. • **msg** *msg*: A specified message is displayed after successful user logout. The default value is **LogoutSuccess!**. • **redirect-url** *redirect-url*: A user is redirected to a specified URL after 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 200 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

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 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**

 Copyright © Huawei Technologies Co., Ltd.

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 or GET 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
```

19.6.80 force-push

Function

The **force-push** command enables the forcible URL template or URL push function.

The **undo force-push** command disables the forcible URL template or URL push function.

By default, the forcible URL template or URL push function is disabled.

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.	It is a string of 1 to 200 case-sensitive characters that do not contain spaces and question marks (?). When double quotation marks are used around the string, spaces are allowed in the string.

Views

AAA domain view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After a user is successfully authenticated, the device forcibly redirect the user to a web page when receiving the HTTP or HTTPS packet from the user who accesses web pages for the first time. In addition to pushing advertisement pages, the device can obtain user terminal information through the HTTP or HTTPS packets sent by the users, and apply the information to other services. There are two ways to push web pages:

1. URL: pushes the URL corresponding to the web page.
2. URL template: pushes the URL template. A URL template must be created. The URL template contains the URL of the pushed web page and URL parameters.

Prerequisites

The URL configured using the **19.6.142 url (URL template view)** command in the URL template view cannot be a redirection URL; otherwise, the command does not take effect.

Precautions

If an application program that actively sends HTTP or HTTPS packets is installed on the user terminal, the terminal has sent the HTTP or HTTPS packet before the user accesses a web page. Therefore, the user is unaware of the web page push process.

For HTTP and HTTPS packets, the forcible push function takes effect only when a redirection ACL is used. If the user table always contains redirection ACLs, a web page is forcibly pushed when HTTPS packets from users match redirection ACL rules. Usually, you can configure the RADIUS server to authorize the Huawei extended RADIUS attribute **HW-Redirect-ACL** to users for redirection ACL implementation.

A pushed URL configured in a domain need 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 **19.6.29 display access-user** command output displays the pushed URL, but the browser of the user cannot redirect to the pushed URL .

Example

Push the URL template **abc** in the domain **huawei**.

```
<Huawei> system-view
[Huawei] url-template name abc
[Huawei-url-template-abc] quit
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] force-push url-template abc
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.81 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

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

 Copyright © Huawei Technologies Co., Ltd.

- 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.

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
```

19.6.82 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.83 mac-access-profile (system view)** command.

Follow-up Procedure

Run the **19.6.26 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 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
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.83 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*

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.82 mac-access-profile (authentication profile view)** command in the authentication profile view to bind the authentication profile to a MAC access profile.

Precautions

- The device supports a maximum of 8 configurable MAC access profiles. 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
```

Related Topics

19.6.38 display mac-access-profile configuration

 Copyright © Huawei Technologies Co., Ltd.

19.6.84 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.

 Copyright © Huawei Technologies Co., Ltd.

- CHAP is a three-way handshake authentication protocol. It transmits only user names but not passwords in RADIUS packets. CHAP is more secure and reliable than PAP. If high security is required, CHAP is recommended.

By default, the authentication mode for MAC address authentication is set to PAP. The authentication mode can be changed to CHAP for higher security.

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
```

19.6.85 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.

Format

mac-authen domain *isp-name* **mac-address** *mac-address* **mask** *mask*

undo mac-authen domain [*isp-name*] **mac-address** *mac-address*

undo mac-authen domain mac-address all

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 (--).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mac-address *mac-address*	Specifies an authentication domain for the MAC address authentication user with a specified MAC address.	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

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.

Precautions

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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the **huawei** domain as the authentication domain for the MAC address authentication user with the MAC address 00e0-fc09-bcf9 and MAC address mask ffff-ffff-ffff in the system view.

```
<Huawei> system-view
[Huawei] mac-authen domain huawei mac-address 00e0-fc09-bcf9 mask ffff-ffff-ffff
```

19.6.86 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.

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

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

In the MAC access profile **m1**, set the MAC address to 0002-0002-0002 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 0002-0002-0002 mask 24
```

19.6.87 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

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Set the maximum number of authentication failures within 60 seconds to 4.

```
<Huawei> system-view
[Huawei] mac-authen quiet-times 4
```

19.6.88 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 a unicast MAC address in H-H-H format, where H can be one to four hexadecimal digits.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **19.6.89 mac-authen reauthenticate**.

The **mac-authen reauthenticate mac-address** and **19.6.89 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 **19.6.89 mac-authen reauthenticate** command configures the device to re-authenticate all online MAC address authentication users at intervals.

Example

Enable re-authentication for an online MAC address authentication user with the MAC address 0001-0002-0003.

```
<Huawei> system-view
[Huawei] mac-authen reauthenticate mac-address 0001-0002-0003
```

19.6.89 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

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.91 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.

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
```

Related Topics

19.6.38 display mac-access-profile configuration

19.6.90 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.87 mac-authen quiet-times** command), the device discards the user's MAC address authentication request packets for a period to avoid frequent authentication failures.

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
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.91 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 60 to 7200, 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 **19.6.89 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

 Copyright © Huawei Technologies Co., Ltd.

used and a short re-authentication interval is used, the CPU usage may become high.

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
```

Related Topics

19.6.89 mac-authen reauthenticate

19.6.38 display mac-access-profile configuration

19.6.92 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

 Copyright © Huawei Technologies Co., Ltd.

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.

For detailed configuration of IPSG, see **IPSG Configuration** in the *Huawei AR Series V200R010 Configuration Guide - Security*.

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.
- 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.93 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*]] }

undo mac-authen username [**fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]]]

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password cipher *password*	Specifies the password in cipher text for MAC address authentication. ● If no password is set when a fixed user name is used, the user can log in without a password. This brings a security risk 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 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 six characters.

 Copyright © Huawei Technologies Co., Ltd.

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 (-), 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	Indicates that the name of a MAC address authentication user is in uppercase.	-

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.

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

 Copyright © Huawei Technologies Co., Ltd.

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 WLAN-ESS interface, passwords must be configured.

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
```

Related Topics

19.6.38 display mac-access-profile configuration

19.6.94 nginx proxy port

Function

The **nginx proxy port** command configures the port number of the Nginx proxy server.

The **undo nginx proxy port** command deletes the port number of the Nginx proxy server.

By default, the port number is 81 configured for the Nginx proxy server.

NOTE

Only the AR161EW, AR161EW-M1, AR169EGW-L, and AR169EW support the Nginx server.

Format

nginx proxy port { **default** | *port-number* }

undo nginx proxy port

Parameters

Parameter	Description	Value
default	Specifies the default port for the Nginx proxy server. **NOTE** The default port number is 81.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port-number	Specifies the port number for the Nginx proxy server. **NOTE** The configured port number must be the same as the Nginx port number included in the Nginx configuration file.	The value is an integer that ranges from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The AR router has a built-in Nginx server, which functions as a web server. The server supports independent portal authentication of the router as well as provides web service to the mobile terminals of passengers. To configure the port number for the Nginx proxy server, run the **nginx proxy port** command. When an AR receives an HTTP request packet from a user to the Internet, traffic is forwarded to the interface where Nginx server is enabled. Then the Nginx server provides services such as web service to users.

Precautions

- Before using this command, run the **ngnix enable** command to enable the Nginx server.
- The configured port number must be the same as the Nginx port number included in the Nginx configuration file.

Example

Set the port number of Ngnix proxy server to 100.

```
<Huawei> system-view
[Huawei] nginx proxy port 100
```

19.6.95 nginx enable

Function

The **nginx enable** command enables the Nginx server.

The **undo nginx enable** command disables the Nginx server.

By default, the Nginx server is disabled.

NOTE

Only the AR161EW, AR161EW-M1, AR169EGW-L, and AR169EW support the Nginx server.

 Copyright © Huawei Technologies Co., Ltd.

Format

nginx enable

undo nginx enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The routers have an embedded Nginx server. The Nginx server functions as a web server to provide web services for passengers through mobile terminals and a running environment for the Portal authentication function.

By default, the Nginx server is disabled on a started device. You can run the **nginx enable** command to enable the Nginx server.

Precautions

The Nginx configuration file must be in correct format and successfully loaded; otherwise, the Nginx server cannot be enabled.

Example

Enable the Nginx server.

```
<Huawei> system-view
[Huawei] nginx enable
Info: Nginx has been started.
```

19.6.96 nginx load

Function

The **nginx load** command configures the device to load the Nginx configuration file to the Nginx server when the server is enabled.

NOTE

The Nginx configuration file has a name extension **.conf**.

Format

nginx load { **default** | *file-name* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
default	Loads the default Nginx configuration file.	-
file-name	Loads the Nginx configuration file stored in the specified directory of a storage medium, such as the flash memory and SD card. **NOTE** If you specify only the file name but not the directory, the device loads the Nginx configuration file in the current storage directory (root directory of the flash memory).	The value is a character string of 6 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The Nginx configuration file defines web services provided by the Nginx server. Usually, a default Nginx configuration file is placed in the configuration directory of the routers before delivery and defines basic web services. When the Nginx server is enabled for the first time, the device loads the default Nginx configuration file to the Nginx server.

If you expect to extend web services provided by the Nginx server, place a new Nginx configuration file in the flash memory or SD card and then run the **nginx load** *file-name* command to load the configuration file to the Nginx server.

Precautions

- After the **nginx load** *file-name* command is run, the loaded Nginx configuration file is protected in the flash memory or SD card and cannot be modified or deleted.
- If you repeatedly load Nginx configuration files of different names in the system view, only the latest configuration file takes effect.
- After the Nginx configuration file is successfully loaded, run the **undo nginx enable** and **nginx enable** command in sequence to enable the Nginx server and make the configuration file take effect.

 Copyright © Huawei Technologies Co., Ltd.

- If you restart the device without saving configurations, the Nginx server still uses the last loaded configuration file on restart.

NOTE

Only the AR161EW, AR161EW-M1, AR169EGW-L, and AR169EW support the Nginx server.

Example

Load the default Nginx configuration file.

```
<Huawei> system-view
[Huawei] nginx load default
Info: Load nginx config file successful.
[Huawei] nginx enable
Info: Nginx has been started.
```

Load the Nginx configuration file in the root directory of the flash memory.

```
<Huawei> cd flash:
<Huawei> system-view
[Huawei] nginx load test.conf
Info: Load nginx config file successful.
[Huawei] undo nginx enable
[Huawei] nginx enable
Info: Nginx has been started.
```

19.6.97 parameter

Function

The **parameter** command sets the characters used in URL.

The **undo parameter** command restores the default settings.

By default, the start character is ?, assignment character is =, and delimiter is &.

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*	Changes the specified start character to ?.	The value is one case-sensitive character without spaces.
assignment-mark *parameter-value*	Specifies the assignment character of the URL parameters.	The value is one case-sensitive character without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
isolate-mark *parameter-value*	Specifies the delimiter between URL parameters.	The value is one case-sensitive character without spaces.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

The **parameter** command allows you to customize the characters in URL.

For example, if the URL configured using the **19.6.142 url (URL template view)** command in the URL template bound to a Portal server profile is http://10.1.1.1, you can run the **19.6.145 url-parameter** command to add the user MAC address, user IP address, and device system name to the URL by specifying the **user_mac**, **user_ip**, and **device** parameters.

When a user with IP address 10.1.1.11 and MAC address 0002-0002-0002 connects to an access device **huawei**, the access device redirects the user to http://10.1.1.1?user_mac=0002-0002-0002&user_ip=10.1.1.11&device=huawei for Portal authentication. In the redirection URL, ? is the default start character, = is the default assignment character, & is the delimiter between parameters.

NOTE

If *parameter-value* is set to a question mark (?) in the URL, the command cannot be executed.

Example

Change the start character in a URL from # to ?.

```
<Huawei> system-view
[Huawei] url-template name huawei
[Huawei-url-template-huawei] parameter start-mark #
```

19.6.98 port (Portal server profile 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.

 Copyright © Huawei Technologies Co., Ltd.

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 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server profile on the device using the **19.6.157 web-auth-server (system view)** 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

 Copyright © Huawei Technologies Co., Ltd.

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 profile **huawei**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] port 10000
```

Related Topics

19.6.52 display web-auth-server configuration
19.6.157 web-auth-server (system view)

19.6.99 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.	-

 Copyright © Huawei Technologies Co., Ltd.

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-acces-profile-p1] portal auth-network 10.1.1.0 24
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.100 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.

Format

portal captive-adaptive enable

undo portal captive-adaptive enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Since WLANs are widely provided, users have a demand for quick and convenient authentication by using applications on mobile terminals, without entering user names and passwords. In such authentication mode, mobile terminals need to automatically display the application-based Portal authentication page and the applications need to communicate with the background server. Therefore, the mobile terminals must be connected to the WLANs during authentication.

iOS terminals such as iPhones, iPads, and iMac computers provide the CNA function. This function automatically detects the network connection status after iOS terminals connect to WLANs. If the network is disconnected, the iOS terminals display a page prompting users to enter user names and passwords. If users do not enter the user names and passwords, the iOS terminals automatically disconnect from the WLANs. As a result, users cannot use applications on iOS terminals for authentication.

To solve the problem, enable the CNA adaptive function so that iOS terminals are redirected to the application-based Portal authentication page when they connect to WLANs. Users can click the link on the page to start specified applications to perform Portal authentication. If users do not start applications to perform authentication, they can still access authentication-free resources on the WLANs.

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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the CNA adaptive function for iOS terminals.

```
<Huawei> system-view
[Huawei] portal captive-adaptive enable
```

19.6.101 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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

19.6.102 portal https-redirect enable

Function

The **portal https-redirect enable** command enables HTTPS redirection of Portal authentication.

The **undo portal https-redirect enable** command disables HTTPS redirection of Portal authentication.

By default, HTTPS redirection of Portal authentication is disabled.

Format

portal https-redirect enable

undo portal https-redirect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Many well-known websites such as Google and Baidu use Hypertext Transfer Protocol Secure (HTTPS). When users visit these websites, it is required that users should be redirected to the Portal authentication page so that Portal authentication can be performed and the users can normally access the network. If unauthenticated Portal users visit websites using HTTPS after HTTPS redirection of Portal authentication is enabled, the device can redirect the users to the Portal authentication page.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- If Portal authentication is triggered when a user visits a website using HTTPS, the browser displays a security prompt. The user needs to click **Continue** to complete Portal authentication.
- Redirection cannot be performed for browsers or websites using HTTP Strict Transport Security (HSTS).
- If the destination port in HTTPS request packets sent by users is an unknown port (443), redirection cannot be performed.
- This function takes effect only for new Portal authentication users.
- This function takes effect only after the Portal server template is created or the IP address of the built-in Portal server is configured.

Example

Enable HTTPS redirection of Portal authentication.

```
<Huawei> system-view
[Huawei] portal https-redirect enable
```

19.6.103 portal local-server ad-image load

Function

The **portal local-server ad-image load** command loads an advertisement image file to the built-in Portal server login page.

The **undo portal local-server ad-image load** command deletes the advertisement image file loaded to the built-in Portal server login page.

By default, no advertisement image file is loaded to the built-in Portal server login page.

Format

portal local-server ad-image load *ad-image-file*

undo portal local-server ad-image load

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ad-image-file	Specifies the name of an advertisement image file to be loaded to the built-in Portal server login page. The size of the advertisement image file must be equal to or less than 256 KB. A file of 670 x 405 pixels is recommended.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. • *drive*: indicates the storage device name. • *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". • *filename*: indicates the file name. The jpg and png formats are supported, and the file name extension must be .jpg, .jpeg, or .png. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a blank area on the login page of the default page package used by the built-in Portal server. Users can customize this area by loading an advertisement image file. When the login page needs to be customized based on special requirements, the administrator can upload the user-defined advertisement image file to the device and run the **portal local-server ad-image load** command. After the advertisement image file is loaded, the user-defined advertisement images are displayed on the built-in Portal server login page for authentication.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The user-defined advertisement image file has been uploaded to the device.

Example

Load the advertisement image file **ad.png** to the built-in Portal server login page.

```
<Huawei> system-view
[Huawei] portal local-server ad-image load flash:/ad.png
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

Related Topics

19.6.43 display portal local-server

19.6.104 portal local-server authentication-method

Function

The **portal local-server authentication-method** command configures the authentication mode for Portal users on the built-in Portal server.

The **undo portal local-server authentication-method** command restores the default authentication mode for Portal users on the built-in Portal server.

By default, the built-in Portal server uses CHAP to authenticate Portal users.

Format

portal local-server authentication-method { **chap** | **pap** }

undo portal local-server authentication-method

Parameters

Parameter	Description	Value
chap	Indicates that the built-in Portal server uses CHAP to authenticate Portal users.	-
pap	Indicates that the built-in Portal server uses PAP to authenticate Portal users.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Password Authentication Protocol (PAP) is a two-way handshake authentication protocol. It transmits passwords in plain text format in RADIUS packets.

Challenge Handshake Authentication Protocol (CHAP) is a three-way handshake authentication protocol. It transmits only user names using RADIUS packets, but does not transmit passwords. CHAP is more secure and reliable than PAP. If high security is required, CHAP is recommended.

Prerequisites

The built-in Portal server function has been enabled globally using the **portal local-server** command.

Example

Configure the built-in Portal server to use PAP to authenticate Portal users.

```
<Huawei> system-view
[Huawei] portal local-server authentication-method pap
```

19.6.105 portal local-server background-color

Function

The **portal local-server background-color** command configures the background color of the built-in Portal server login page.

The **undo portal local-server background-color** command cancels the background color configured for the built-in Portal server login page.

By default, no background color of the built-in Portal server login page is configured.

Format

portal local-server background-color *background-color-value*

undo portal local-server background-color

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
background-color-value	Specifies the background color of the built-in Portal server login page.	The value is a string that ranges from #000000 to #FFFFFF in the RGB format. The hexadecimal code is used to indicate the page color, and the format is always #DEFABC (A-F and 0-9).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Users can customize the login page of the default page package used by the built-in Portal server. The administrator can configure the background color of the login page.

Example

Configure the user-defined background color of the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server background-color #AABBCC
```

19.6.106 portal local-server background-image load

Function

The **portal local-server background-image load** command loads a background image file to the built-in Portal server login page.

The **undo portal local-server background-image load** command deletes the background image file loaded to the built-in Portal server login page.

By default, the device has two background images **default-image0** and **default-image1**. The built-in Portal server uses **default-image0** as the background image by default.

Format

portal local-server background-image load { *background-image-file* | **default-image1** }

 Copyright © Huawei Technologies Co., Ltd.

undo portal local-server background-image load

Parameters

Parameter	Description	Value
background-image-file	Specifies the name of the background image file to be loaded to the built-in Portal server login page. The size of the background image file must be equal to or less than 512 KB. A file of 1366 x 768 pixels is recommended.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". ● *filename*: indicates the file name. The jpg and png formats are supported, and the file name extension must be .jpg, .jpeg, or .png. If you enter only the file name, the system considers that the file is stored in the default directory.
default-image1	Loads the background image **default-image1** to the built-in Portal server login page.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

Users can customize the login page of the default page package used by the built-in Portal server. Users can customize background images or select the default ones. When the background image of the login page needs to be customized based on special requirements, the administrator can upload the user-defined background image file to the device and run the **portal local-server background-image load** command. After the image is loaded, the user-defined background image file is displayed on the built-in Portal server login page for authentication.

Prerequisites

The user-defined background image has been uploaded to the device.

Example

Load the background image file **bg.png** to the built-in Portal server login page.

```
<Huawei> system-view
[Huawei] portal local-server background-image load flash:/bg.png
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

19.6.107 portal local-server enable

Function

The **portal local-server enable** command enables the built-in Portal server function in a Portal access profile.

The **undo portal local-server enable** command restores the default setting.

By default, the built-in Portal server function is disabled in a Portal access profile.

Format

portal local-server enable [**layer3**]

undo portal local-server enable

Parameters

Parameter	Description	Value
layer3	Indicates Layer 3 built-in Portal authentication. If this parameter is not specified, Layer 2 built-in Portal authentication is used.	-

Views

Portal access profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Portal authentication, the device needs to provide the IP address of the Portal server. The device supports external and built-in Portal servers. When the built-in Portal server is required to authenticate users, enable the built-in Portal server function globally and then run the **portal local-server enable** command in the Portal access profile. Then the built-in Portal server can be used to authenticate the users who use the Portal access profile.

Portal authentication can work either in Layer 2 or Layer 3 mode.

- In Layer 2 mode, there is no Layer 3 forwarding device between a device and a user. The device can learn the user's MAC address and identify the user using both the user's IP and MAC addresses.
- In Layer 3 mode, there is a Layer 3 forwarding device between a device and a user. The device cannot learn the user's MAC address and has to identify the user using the user's IP address.

Prerequisites

The built-in Portal server function has been enabled globally using the **19.6.112 portal local-server** command.

Example

In the Portal access profile **p1**, enable the built-in Portal server function.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] ip address 10.1.1.1 24
[Huawei-LoopBack1] quit
[Huawei] portal local-server ip 10.1.1.1
[Huawei] ssl policy s1 type server
[Huawei-ssl-policy-s1] pki-realm default
[Huawei-ssl-policy-s1] quit
[Huawei] http secure-server ssl-policy s1
[Huawei] portal local-server https ssl-policy s1
[Huawei] portal-access-profile name p1
[Huawei-portal-acces-profile-p1] portal local-server enable
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.108 portal local-server ip

Function

The **portal local-server ip** command configures an IP address for the built-in Portal server.

The **undo portal local-server ip** command deletes an IP address of the built-in Portal server.

 Copyright © Huawei Technologies Co., Ltd.

By default, no IP address is configured for the built-in Portal server.

Format

portal local-server ip *ip-address*

undo portal local-server ip

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the built-in Portal server.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device is used as a built-in Portal server, you can run the **portal local-server ip** command to configure an IP address for the built-in Portal server. Users are then redirected to the Portal server if they enter URLs that are not located in the free IP subnet.

NOTE

- The IP address assigned to the built-in Portal server must have a reachable route to the user.
- It is recommended that a loopback interface address be assigned to the built-in Portal server because the loopback interface is stable. Additionally, packets destined for loopback interfaces are not sent to other interfaces on the network; therefore, system performance is not deteriorated even if many users request to go online.
- After users go online through the built-in Portal server, if the interface address or interface (non-physical interface) matching the built-in Portal server's IP address is deleted, online users cannot go offline and offline users cannot go online. Therefore, exercise caution when you delete the interface address or interface.

Example

Assign the IP address 10.1.1.1 to the built-in Portal server.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] ip address 10.1.1.1 24
[Huawei-LoopBack1] quit
[Huawei] portal local-server ip 10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.109 portal local-server keep-alive

Function

The **portal local-server keep-alive** command configures the heartbeat detection interval and mode of the built-in Portal server.

The **undo portal local-server keep-alive** command cancels the configured heartbeat detection interval and mode of the built-in Portal server.

By default, the heartbeat detection function of the built-in Portal server is not configured.

Format

portal local-server keep-alive interval *interval-value* [**auto**]

undo portal local-server keep-alive

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the heartbeat detection interval of the built-in Portal server.	The value is an integer that ranges from 30 to 7200, in seconds.
auto	Specifies the automatic detection mode. If this parameter is not configured, the forcible detection mode is specified.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user closes the browser or an exception occurs, the device can detect the user's online state to determine whether to make the user go offline. The administrator can configure the heartbeat detection function of the built-in Portal server. If the device does not receive a heartbeat packet from the client within a specified period, the user is specified to go offline. The heartbeat detection mode of the built-in Portal server can be either of the following modes:

 Copyright © Huawei Technologies Co., Ltd.

- Forcible detection mode: This mode is valid for all users. If the device does not receive a heartbeat packet from a user within a specified period, the device specifies the user to go offline.
- Automatic detection mode: The device checks whether the client browser supports the heartbeat program. If yes, the forcible detection mode is used for the user; if no, the device does not detect the user. You are advised to configure this mode to prevent users from going offline because the browser does not support the heartbeat program.

  NOTE

  Currently, the heartbeat program is supported by Internet Explorer 8, FireFox 3.5.2, Chrome 28.0.1500.72, and Opera 12.00 on Windows 7. A Java program must be installed and configured on the operating system.

  Browsers using Java1.7 and later versions do not support the heartbeat program.

Precautions

When the forcible detection mode is configured, the device specifies users to go offline to prevent from failing to receive heartbeat packets for a long time during network congestion. In this scenario, the heartbeat detection interval must be increased.

If you run this command multiple times in the same view, only the latest configuration takes effect.

Example

Configure the automatic detection function of the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server keep-alive interval 60 auto
```

19.6.110 portal local-server load

Function

The **portal local-server load** command loads a page file package to the built-in Portal server.

The **undo portal local-server load** command restores the default configuration.

By default, the built-in Portal server loads the default page file package **portalpage.zip**.

Format

portal local-server load *string*

undo portal local-server load

Parameters

Parameter	Description	Value
string	Specifies the name of the page file package to be loaded to the built-in Portal server.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. • *drive*: indicates the storage device name. • *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". • *filename*: indicates the file name. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Customized page file packages can be loaded to the built-in Portal server.

Prerequisites

The page file (.zip) has been uploaded from the PC to the device storage media.

Precautions

The default page file package can be modified but cannot be deleted. If it is deleted, the built-in Portal server fails to load the pages after startup.

This function is used by technical support personnel to develop limited page customization based on customer requirements and does not apply to customization by customers themselves.

 Copyright © Huawei Technologies Co., Ltd.

Example

Load the page file **portalpage_01.zip** on the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server load portalpage_01.zip
Warning: Portal local server has been enabled, and this operation will affect online user, continue?[Y/N]:y
```

Related Topics

19.6.44 display portal local-server page-information

19.6.43 display portal local-server

19.6.111 portal local-server logo load

Function

The **portal local-server logo load** command loads a logo file to the built-in Portal server login page.

The **undo portal local-server logo load** command deletes the logo file loaded to the built-in Portal server login page.

By default, no logo file is loaded to the built-in Portal server login page.

Format

portal local-server logo load *logo-file*

undo portal local-server logo load

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
logo-file	Specifies the name of the logo file to be loaded to the built-in Portal server login page. The size of the logo file must be equal to or less than 128 KB. A file of 591 x 80 pixels is recommended.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. • *drive*: indicates the storage device name. • *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". • *filename*: indicates the file name. The jpg and png formats are supported, and the file name extension must be .jpg, .jpeg, or .png. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a blank area on the login page of the default page package used by the built-in Portal server. Users can customize this area by loading a logo file. When the login page needs to be customized based on special requirements, the administrator can upload the user-defined logo file to the device and run the **portal local-server logo load** command. After the logo file is loaded, the user-defined logo is displayed on the built-in Portal server login page for authentication.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The user-defined logo file has been uploaded to the device.

Example

Load the logo file **logo.png** to the built-in Portal server login page.

```
<Huawei> system-view
[Huawei] portal local-server logo load flash:/logo.png
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

Related Topics

19.6.43 display portal local-server

19.6.112 portal local-server

Function

The **portal local-server** command enables the built-in Portal server function.

The **undo portal local-server** command disables the built-in Portal server function.

By default, the built-in Portal server function is disabled.

Format

portal local-server https ssl-policy *policy-name* [**port** *port-num*]

undo portal local-server https

Parameters

Parameter	Description	Value
https	Configures the built-in Portal server to exchange authentication messages with users using the Hypertext Transfer Protocol Secure (HTTPS) protocol.	-
ssl-policy *policy-name*	Specifies the Secure Sockets Layer (SSL) policy used by the built-in Portal server.	The value must be the name of an existing SSL policy.
port *port-num*	Specifies the TCP port number used. If you do not specify a port number, the default port number is used.	The value can be 443 or any integer in the range of 1025 to 55535. By default, the port number is 443.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with an external Portal server, a built-in Portal server is easy to use, cost-effective, and easy to maintain. After a built-in Portal server is configured, Portal authentication can be implemented for users without an external Portal server. When using the **portal local-server** command to enable the built-in Portal server function, configure the built-in Portal server to exchange authentication messages with users using the HTTPS protocol. HTTPS is a secure extension of HTTP and uses the SSL protocol to guarantee secure communication. To enable the built-in Portal server to exchange authentication messages using HTTPS, you need to configure an SSL policy and load a digital certificate to the server.

Prerequisites

- The IP address of the built-in Portal server has been configured using the **19.6.108 portal local-server ip** command.
- An SSL policy has been configured using the **ssl policy** *policy-name* command in the system view
- A server SSL policy has been configured and associated with the HTTPS server using the **19.19.4 http secure-server ssl-policy** command.
- You have obtained a digital certificate for the SSL policy from an authorized certificate authority.

Precautions

When there are Portal authentication users online, you cannot disable the built-in Portal server function or change the SSL policy for the built-in Portal server.

Example

Enable the built-in Portal server function and configure the server to use the SSL policy **s1**.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] ip address 10.1.1.1 24
[Huawei-LoopBack1] quit
[Huawei] portal local-server ip 10.1.1.1
[Huawei] ssl policy s1 type server
[Huawei-ssl-policy-s1] pki-realm default
[Huawei-ssl-policy-s1] quit
[Huawei] http secure-server ssl-policy s1
[Huawei] portal local-server https ssl-policy s1
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.113 portal local-server page-text load

Function

The **portal local-server page-text load** command loads the use instruction page file of the built-in Portal server.

The **undo portal local-server page-text load** command deletes the loaded use instruction page file of the built-in Portal server.

By default, no use instruction page file of the built-in Portal server is loaded.

Format

portal local-server page-text load *string*

undo portal local-server page-text load

Parameters

Parameter	Description	Value
string	Specifies the use instruction page file of the built-in Portal server.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of [drive] [path] filename. • **drive** indicates the storage device name. • **path** indicates the directory or sub-directory. The directory name cannot contain the following characters: ~ * / \ : ' " • **filename** indicates the file name. The file name extension must be .txt or .html. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to customize the use instruction page, you can upload the customized use instruction page file to the device, and run this command to load the file. After the file is loaded, the hyperlink **Instruction for Use** is generated on the login page of the built-in Portal server, and users can click the hyperlink to access the use instruction page.

Prerequisite

The page file to be loaded has been uploaded to the device.

Precautions

When the to-be-loaded page is customized, the page length and width are fixed. After adjusting the page, the administrator must upload and load the modified page again.

Currently, only Chinese or English page files can be loaded on the device.

Example

Load the use instruction page file **page.html** to the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server page-text load flash:/page.html
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

Related Topics

19.6.43 display portal local-server

19.6.114 portal local-server policy-text load

Function

The **portal local-server policy-text load** command loads a disclaimer page file to the built-in Portal server.

The **undo portal local-server policy-text load** command deletes the loaded disclaimer page file.

By default, no disclaimer page file is loaded to the built-in Portal server.

Format

portal local-server policy-text load *string*

undo portal local-server policy-text load

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
string	Specifies the name of the disclaimer page file to be loaded to the built-in Portal server.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. • *drive*: indicates the storage device name. • *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". • *filename*: indicates the file name. The file name extension must be .txt or .html. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To customize a disclaimer page, upload the disclaimer page file to the device and run this command to load the file. After the file is loaded, the hyperlink **Disclaimer** will be displayed on the login page. You can click the link to visit the disclaimer page.

Prerequisite

The disclaimer page file to be loaded has been uploaded to the device.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Currently, only Chinese and English disclaimer page files can be loaded on the device.

Example

Load the disclaimer page file **policy.html** to the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server policy-text load policy.html
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

Related Topics

19.6.43 display portal local-server

19.6.115 portal local-server syslog-limit enable

Function

The **portal local-server syslog-limit enable** command enables the log suppression function for users authenticated through the built-in Portal server.

The **undo portal local-server syslog-limit enable** command disables the log suppression function for users authenticated through the built-in Portal server.

By default, the log suppression function is enabled for users authenticated through the built-in Portal server.

Format

portal local-server syslog-limit enable

undo portal local-server syslog-limit enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device generates logs when users authenticated through the built-in Portal server fail to go online or offline. If a user fails to go online or offline, the user attempts to go online or offline repeatedly, and the device generates a large number of logs within a short time. This results in a high failure rate in the statistics and degrades the system performance. You can run the **portal local-server syslog-limit enable** command to enable the log suppression function for

 Copyright © Huawei Technologies Co., Ltd.

users authenticated through the built-in Portal server. The device then only generates one log if a user fails to go online or offline within a suppression period (configured using the **19.6.116 portal local-server syslog-limit period** command).

Example

Enable the log suppression function for users authenticated through the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server syslog-limit enable
```

19.6.116 portal local-server syslog-limit period

Function

The **portal local-server syslog-limit period** command configures the log suppression period for users authenticated through the built-in Portal server.

The **undo portal local-server syslog-limit period** command restores the default log suppression period.

By default, the log suppression period is 300 seconds for users authenticated through the built-in Portal server.

Format

portal local-server syslog-limit period *value*

undo portal local-server syslog-limit period

Parameters

Parameter	Description	Value
value	Specifies the log suppression period for users authenticated through the built-in Portal server.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device generates logs when users authenticated through the built-in Portal server fail to go online or offline. If a user fails to go online or offline, the user

 Copyright © Huawei Technologies Co., Ltd.

attempts to go online or offline repeatedly, and the device generates a large number of logs within a short time. This results in a high failure rate in the statistics and degrades the system performance. You can enable the log suppression function (configured using the **19.6.115 portal local-server syslog-limit enable** command) for users authenticated through the built-in Portal server. The device then only generates one log if a user fails to go online or offline within a suppression period.

Example

Set the log suppression period to 1000 seconds for users authenticated through the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server syslog-limit period 1000
```

19.6.117 portal local-server timer session-timeout

Function

The **portal local-server timer session-timeout** command configures the session timeout interval for built-in Portal authentication users.

The **undo portal local-server timer session-timeout** command restores the default session timeout interval for built-in Portal authentication users.

By default, the session timeout interval is 8 hours for built-in Portal authentication users.

Format

portal local-server timer session-timeout *interval*

undo portal local-server timer session-timeout

Parameters

Parameter	Description	Value
interval	Specifies the session timeout interval for built-in Portal authentication users.	The value is an integer that ranges from 1 to 720, in hours.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

 Copyright © Huawei Technologies Co., Ltd.

When built-in Portal authentication is used for users and the device functions as a built-in Portal server, you can configure the session timeout interval for the users. The users are disconnected after the specified session timeout interval. To connect to the network again, the users need to be re-authenticated.

Precautions

The session timeout interval for built-in Portal authentication users is calculated based on the device time. For example, if the session timeout interval is 6 hours and the device time is 2014-09-01 02:00:00 when a user was connected, the user should be disconnected at 2014-09-01 08:00:00. Therefore, ensure that the device time and time zone are correct after the session timeout interval is configured for users. If the device time is incorrect, users may fail to be connected or disconnected properly. You can run the **display clock** command to check the device time and the time zone.

Example

Set the session timeout interval to 10 hours for built-in Portal authentication users.

```
<Huawei> system-view
[Huawei] portal local-server timer session-timeout 10
```

Related Topics

19.6.43 display portal local-server

19.6.118 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.6.41 display portal

19.6.119 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** } *

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.6.41 display portal

19.6.48 display portal user-logout

 Copyright © Huawei Technologies Co., Ltd.

19.6.120 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
```

19.6.121 portal quiet-period

Function

The **portal quiet-period** command enables the quiet timer for Portal authentication.

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.122 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 **19.6.123 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
```

19.6.122 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.121 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
```

19.6.123 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.121 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 **19.6.122 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
```

19.6.124 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

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.

Example

In the Portal access profile **p1**, set the offline detection interval of Portal authentication users to 400s.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] portal-access-profile name p1
[Huawei-portal-acces-profile-p1] portal timer offline-detect 400
```

19.6.125 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 **19.6.120 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.6.120 portal max-user

19.6.126 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

Parameters

Parameter	Description	Value
http	Sets the HTTP protocol for Portal authentication. **NOTE** The HTTP protocol poses security risks. The HTTPS protocol is recommended.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 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 **19.6.127 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 type server
[Huawei-ssl-policy-huawei] quit
[Huawei] http secure-server ssl-policy huawei
[Huawei] portal web-authen-server https ssl-policy huawei port 8443
```

Related Topics

19.6.52 display web-auth-server configuration

 Copyright © Huawei Technologies Co., Ltd.

19.6.127 protocol

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. • **none**: The password is not encoded. • **uam**: The password is encoded using ASCII characters.	-
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.

 Copyright © Huawei Technologies Co., Ltd.

- HACA protocol
- Portal protocol
- HTTP or HTTPS protocol

The HACA protocol used in Portal authentication has impacts on other command configurations.

- After the HACA protocol is configured, the following command configurations will not be supported:
  - Run the **19.6.98 port (Portal server profile view)** command to configure a destination port number for the device to send packets to the Portal server.
  - Run the **19.6.135 server-detect** command to enable the Portal server detection function.
  - Run the **19.6.137 shared-key (Portal server profile view)** command to configure a shared key used by the device and Portal server to exchange information.
  - Run the **19.6.139 source-ip (Portal server profile view)** command to configure a source IP address for the device to communicate with the Portal server.
  - Run the **19.6.149 user-sync** command to enable Portal user information synchronization.
  - Run the **19.6.153 vpn-instance (Portal server template view)** command to configure a VPN instance for the device to communicate with the Portal server.

  If any one of the preceding configurations is performed beforehand, the HACA protocol configuration will not take effect.
- After the HACA protocol is configured, you can run the **19.6.136 server-ip (Portal server profile view)** command to configure an IP address for the Portal server. However, if multiple Portal server IP addresses are configured, the HACA protocol configuration will not take effect.

Example

Set the protocol used in Portal authentication to HACA.

```
<Huawei> system-view
[Huawei] web-auth-server abc
[Huawei-web-auth-server-abc] protocol haca
```

19.6.128 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

 Copyright © Huawei Technologies Co., Ltd.

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 redirected 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
```

Related Topics

19.6.47 display portal url-encode configuration

19.6.129 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.

 Copyright © Huawei Technologies Co., Ltd.

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 has been configured for the Portal access profile:

- If the external Portal server is used, the Portal server profile used by the Portal access profile has been configured using the **19.6.155 web-auth-server (Portal access profile view)** command.
- If the built-in Portal server is used, the built-in Portal server function of the Portal access profile has been enabled using the **19.6.107 portal local-server enable** command.

Follow-up Procedure

Run the **19.6.26 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.

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.130 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

 Copyright © Huawei Technologies Co., Ltd.

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

Configure the portal server used by the portal access profile:

- If the external portal server is used, run the **19.6.155 web-auth-server (Portal access profile view)** command to configure the portal server profile for the portal access profile.
- If the built-in portal server is used, run the **19.6.107 portal local-server enable** command to configure the built-in portal server function for the portal access profile.

Precautions

- The device supports a maximum of 8 configurable portal access profiles. 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
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.131 redirect web-authentication-user

Function

The **redirect web-authentication-user** command enables the device to redirect Portal authentication users to the built-in Portal server after 3G/LTE links are disconnected.

The **undo redirect web-authentication-user** command disables the device from redirecting Portal authentication users to the built-in Portal server after 3G/LTE links are disconnected.

 Copyright © Huawei Technologies Co., Ltd.

By default, the device does not redirect Portal authentication users to the built-in Portal server after 3G/LTE links are disconnected.

Format

redirect web-authentication-user url *url-string*

undo redirect web-authentication-user

Parameters

Parameter	Description	Value
url *url-string*	Specifies the URL address of a built-in Portal server. A URL identifies the Portal server's website that Portal authentication users can access. A URL is easier to remember than an IP address.	The value is a string of 1 to 200 case-sensitive characters without spaces and question marks (?). If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When routers are deployed as mobile Internet gateways on buses and subways, users can connect to the vehicle-mounted Wi-Fi network and access the Internet through the 3G/LTE interfaces after they pass Portal authentication. If 3G/LTE links are disconnected, users cannot access any page, degrading user experiences.

You can run the **redirect web-authentication-user** command on 3G/LTE interfaces to enable the device to redirect Portal authentication users to the built-in Portal server after 3G/LTE links are disconnected. In this way, users can access server resources, improving user experience.

Precautions

- The **redirect web-authentication-user** and **cut web-authentication-user** commands cannot be configured simultaneously on the same interface. It is recommended that either **redirect web-authentication-user** or **cut web-authentication-user** be configured on different interfaces of the same device.

 Copyright © Huawei Technologies Co., Ltd.

- If the **redirect web-authentication-user** command is configured on multiple cellular interfaces, ensure that the URLs configured on these interfaces are the same.
- After all 3G/LTE uplinks are disconnected, the device redirects Portal authentication users to the built-in Portal server.

Example

Redirect Portal authentication users to the built-in Portal server with the URL http://192.168.10.1 after 3G/LTE links are disconnected.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] redirect web-authentication-user url http://192.168.10.1
```

Related Topics

19.6.28 cut web-authentication-user

19.6.132 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.

Format

remark { **8021p** *8021p-value* | **dscp** *dscp-value* | **exp** *exp-value* | **lp** *lp-value* } *

undo remark { **8021p** *8021p-value* | **dscp** *dscp-value* | **exp** *exp-value* | **lp** *lp-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.
exp *exp-value*	Specifies the priority for processing MPLS packets.	The value is an integer that ranges from 0 to 7.
lp *lp-value*	Specifies the priority for processing internal packets in the device.	The value is an integer that ranges from 0 to 7.

 Copyright © Huawei Technologies Co., Ltd.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

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.

NOTE

When an AR router is connected to Fit APs, the user group priority configuration does not take effect for users who go online from the Fit APs.

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
```

Related Topics

19.6.150 user-group

19.6.133 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*] } &<1-5>]

 Copyright © Huawei Technologies Co., Ltd.

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 **19.6.32 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 **19.6.32 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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.6.32 display dot1x

19.6.134 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 **19.6.39 display mac-authen** command to check whether the authentication function is normal.

Copyright © Huawei Technologies Co., Ltd.

- 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 **19.6.39 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
```

Related Topics

19.6.39 display mac-authen

19.6.135 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** } *] *

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 16. The default value is 0. The default value is recommended.

 Copyright © Huawei Technologies Co., Ltd.

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 profile 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 profile, the device detects all Portal servers configured in the Portal server profile. 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

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 profile **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
```

Related Topics

19.6.149 user-sync

19.6.136 server-ip (Portal server profile 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>

undo server-ip { *server-ip-address* | **all** }

Parameters

Parameter	Description	Value
server-ip-address	Specifies an IP address of a Portal server.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Deletes all IP addresses of a Portal server.	-

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server profile on the device using the **19.6.157 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 profile 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 profile. 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 profile, users are allowed to access the IP address.
- If multiple IP addresses are configured for a Portal server in the Portal server profile, you are advised to run the **19.6.143 url (Portal server profile 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.

Example

Set the Portal server IP address in the Portal server profile **huawei** to 10.10.10.1.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] server-ip 10.10.10.1
```

Related Topics

19.6.52 display web-auth-server configuration

 Copyright © Huawei Technologies Co., Ltd.

19.6.137 shared-key (Portal server profile 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 16 characters in plain text, or a string of 48 characters in cipher text. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Portal server profile 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

 Copyright © Huawei Technologies Co., Ltd.

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 6 characters.

Example

Configure the shared key in the Portal server profile **huawei** to **huawei@123**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] shared-key cipher huawei@123
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.138 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

 Copyright © Huawei Technologies Co., Ltd.

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 huawei
[Huawei-web-auth-server-huawei] source-interface loopback 1
```

19.6.139 source-ip (Portal server profile 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

 Copyright © Huawei Technologies Co., Ltd.

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 profile 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 profile 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, all 1s, 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 profile **huawei**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] source-ip 192.168.1.100
```

19.6.140 snmp-agent trap enable feature-name mid_eapol

Function

The **snmp-agent trap enable feature-name mid_eapol** command enables the trap function for the DOT1X module.

The **undo snmp-agent trap enable feature-name mid_eapol** command disables the trap function for the DOT1X module.

By default, the trap function is enabled for the DOT1X module.

 Copyright © Huawei Technologies Co., Ltd.

Format

snmp-agent trap enable feature-name mid_eapol [**trap-name** { **hwmacauthenmaxuseralarm** | **hwsrvcfgeapmaxuseralarm** }]

undo snmp-agent trap enable feature-name mid_eapol [**trap-name** { **hwmacauthenmaxuseralarm** | **hwsrvcfgeapmaxuseralarm** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event of the DOT1X module.	-
hwmacauthenmaxuser-alarm	Enables the device to send a Huawei proprietary trap when the number of MAC address authentication users reaches the maximum number allowed on an interface.	-
hwsrvcfgeapmaxusera-larm	Enables the device to send a Huawei proprietary trap when the number of 802.1X authentication users reaches the maximum number allowed on an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** to enable the trap function for one or more events.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the trap function for hwmacauthenmaxuseralarm of the DOT1X module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mid_eapol trap-name hwmacauthenmaxuseralarm
```

Related Topics

19.6.53 display snmp-agent trap feature-name mid_eapol all

19.6.141 snmp-agent trap enable feature-name mid_web

Function

The **snmp-agent trap enable feature-name mid_web** command enables the trap function for the web authentication module.

The **undo snmp-agent trap enable feature-name mid_web** command disables the trap function for the web authentication module.

By default, the trap function is enabled for the web authentication module.

Format

snmp-agent trap enable feature-name mid_web [**trap-name** { **hwportalmaxuseralarm** | **hwportaluserclearalarm** | **hwportalserverdown** | **hwportalserverup** }]

undo snmp-agent trap enable feature-name mid_web [**trap-name** { **hwportalmaxuseralarm** | **hwportaluserclearalarm** | **hwportalserverdown** | **hwportalserverup** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event of the web authentication module.	-
hwportalmaxuseralarm	Enables the device to send a Huawei proprietary trap when the number of online Portal authentication users exceeds the upper threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwportalusercleara-larm	Enables the device to send a Huawei proprietary trap when the number of online Portal authentication users falls below the lower threshold.	-
hwportalserverdown	Enables the device to send a Huawei proprietary trap when it detects that the Portal server changes from Up to Down.	-
hwportalserverup	Enables the device to send a Huawei proprietary trap when it detects that the Portal server changes from Down to Up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** to enable the trap function for one or more events.

Example

Enable the trap function for hwportalmaxuseralarm of the web authentication module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mid_web trap-name hwportalmaxuseralarm
```

Related Topics

19.6.54 display snmp-agent trap feature-name mid_web all

 Copyright © Huawei Technologies Co., Ltd.

19.6.142 url (URL template view)

Function

The **url** command configures the redirection URL or pushed URL.

The **undo url** command cancels the redirection URL or pushed URL.

By default, no redirection URL or pushed URL is configured.

Format

url [**push-only** | **redirect-only**] *url-string* [**ssid** *ssid*]

undo url [**push-only** | **redirect-only**] [**ssid** *ssid*]

Parameters

Parameter	Description	Value
url-string	Specifies the redirection URL or pushed URL.	It is a string of 1 to 200 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
push-only	Specifies the URL as a pushed URL.	-
redirect-only	Specifies the URL as a redirection URL.	-
ssid *ssid*	Specifies the SSID that users associate with. This parameter is only valid 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

 Copyright © Huawei Technologies Co., Ltd.

After a URL template is created using the **19.6.147 url-template name** command, you can run this command to configure the redirection URL or pushed URL. The difference between redirection URL and pushed URL is as follows.

- Redirection URL: When a user without network access right connects to the network, the Portal authentication device redirects the user to the redirection 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

If the **push-only** and **redirect-only** parameters are not specified, the configured URL is used as both redirection URL and pushed URL. You can configure pushed URL using the **19.6.80 force-push** command, or use the **19.6.148 url-template (Portal server profile view)** command to bind a URL template to the Portal server profile to configure redirection URL.

Example

Set the redirection URL to http://10.1.1.1.

```
<Huawei> system-view
[Huawei] url-template name huawei
[Huawei-url-template-huawei] url http://10.1.1.1
```

19.6.143 url (Portal server profile view)

Function

The **url** command configures the URL for a Portal server.

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

By default, no URL is configured for a Portal server.

Format

url *url-string*

undo url

Parameters

Parameter	Description	Value
url-string	Specifies the URL of a portal server.	It is a string of 1 to 200 case-sensitive characters that do not contain spaces and question marks (?). When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Portal server IP address is configured using the **19.6.136 server-ip (Portal server profile view)** command, the Portal server URL is generated by default on the device. If the existing Portal server URL is inconsistent with the default one or the domain name needs to be used, you need to run the **url** command to specify the Portal server URL.

Precautions

A Portal server only has one URL.

Example

Set the URL of a Portal server to http://www.***.com in the Portal server profile **huawei**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] url http://www.***.com
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.144 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

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
delimiter *delimiter*	Specifies the delimiter in MAC address.	The value is one case-sensitive character without spaces.
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 huawei
[Huawei-url-template-huawei] url-parameter mac-address format delimiter - compact
```

19.6.145 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 parameters.

Format

url-parameter { **ac-ip** *ac-ip-value* | **ac-mac** *ac-mac-value* | **ap-ip** *ap-ip-value* | **ap-mac** *ap-mac-value* | **login-url** *url-key url* | **redirect-url** *redirect-url-value* | **ssid** *ssid-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* | **user-vlan** *user-vlan-value* | **esn** *esn-value* } *

 Copyright © Huawei Technologies Co., Ltd.

undo url-parameter

Parameters

Parameter	Description	Value
ac-ip *ac-ip-value*	Specifies the IP address of the AC 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. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ac-mac *ac-mac-value*	Specifies the MAC address of the AC 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. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ap-ip *ap-ip-value*	Specifies the AP IP address carried in the URL and sets the parameter name. This parameter is only valid for wireless access users.	The value is a string of 1 to 16 case-sensitive characters without spaces. 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. This parameter is only valid for wireless access users.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
login-url *url-key url*	Specifies the login URL of the 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 200 case-sensitive characters without spaces.
redirect-url *redirect-url-value*	Specifies the original URL that a user accesses carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ssid *ssid-value*	Specifies the SSID associated that users associate with carried in the URL and sets the parameter name. This parameter is only valid for wireless access users.	The value is a string of 1 to 16 case-sensitive characters without spaces. 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.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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. 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.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
user-vlan *user-vlan-value*	Specifies the user VLAN carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
esn *esn-value*	Specifies the ESN carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

URL template view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After a URL template is created using the **19.6.147 url-template name** command and URL is configured using the **19.6.142 url (URL template view)** 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 pushed to a website rather than the Portal server according to the URL, the website provides the different web pages for the users according to user terminal information carried in the URL.

Precautions

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 the Agile Controller-Campus.

URL Parameter	URL Parameter Name Supported by the Agile Controller-Campus
ac-ip	ac-ip
ap-mac	apmac
ssid	ssid
redirect-url	url
user-ipaddress	userip
user-mac	usermac

Example

Set the user MAC address and access device system name in the URL.

```
<Huawei> system-view
[Huawei] url-template name huawei
[Huawei-url-template-huawei] url-parameter user-mac usermac sysname huawei
```

19.6.146 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

url-parameter set { **ac-ip** { *ip-address* | **interface** *interface-type interface-number* } | **ap-ip** { *ip-address* | **interface** *interface-type interface-number* } }*

undo url-parameter set { **ac-ip** | **ap-ip** }

Parameters

Parameter	Description	Value
ac-ip	Sets the value of the redirection parameter **ac-ip**.	-
ap-ip	Sets the value of the redirection parameter **ap-ip**.	-
ip-address	Sets the value of a redirection parameter to a specified IP address.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Sets the value of a redirection parameter to the IP address of an interface.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Assume that a URL template is created using the **19.6.147 url-template name** command, and a URL is configured in the URL template using the **19.6.142 url (URL template view)** command. When the device functions as an AC and user terminals communicate with the Portal server, the default value of **ac-ip** is the CAPWAP gateway address and the default value of **ap-ip** is the AP's IP address. When the device functions as a FAT AP and user terminals communicate with the Portal server, the default values of **ac-ip** and **ap-ip** are the user-side gateway address. If clients cannot communicate with the Portal server using the default values, you can run the **url-parameter set** { **ac-ip** { *ip-address* | **interface** *interface-type interface-number* } | **ap-ip** { *ip-address* | **interface** *interface-type interface-number* } }* command to set the value of the redirection parameter **ac-ip** or **ap-ip** (to the IP address of the device's WAN interface generally). 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the value of the redirection parameter **ap-ip** to 10.1.1.1.

```
<Huawei> system-view
[Huawei] url-template name huawei
[Huawei-url-template-huawei] url-parameter set ap-ip 10.1.1.1
```

19.6.147 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 **19.6.157 web-auth-server (system view)** command, you can bind a URL template to the Portal authentication server template. The URL template contains the redirection URL and redirection URL parameters.

The **url-template name** command creates a URL template or displays an existing URL template view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a URL template named **huawei** and enter the template view.

```
<Huawei> system-view
[Huawei] url-template name huawei
```

19.6.148 url-template (Portal server profile view)

Function

The **url-template** command binds a URL template to a Portal server profile.

The **undo url-template** command unbinds a URL template from a Portal server profile.

By default, no URL template is bound to a Portal server profile.

Format

url-template *url-template*

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.

Views

Portal server profile 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 redirection URL.

Prerequisites

A URL template has been created using the **19.6.147 url-template name** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If a URL template is bound to the Portal authentication server template and the **19.6.143 url (Portal server profile view)** command is executed to configure the redirection URL corresponding to the Portal authentication server, only the parameters in the URL template take effect.

The URL configured using the **19.6.142 url (URL template view)** command in the URL template view cannot be a pushed URL; otherwise, the command does not take effect.

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 huawei
[Huawei-web-auth-server-huawei] url-template abc
```

19.6.149 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 profile view

 Copyright © Huawei Technologies Co., Ltd.

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 profile **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
```

19.6.150 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

user-group *group-name* [**group-index** *group-index*]

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: / \ : * ? " < > | @ ' %.
group-index *group-index*	Specifies the index of a user group.	The value is an integer and varies according to device model: • AR100 series, AR120 series, AR150 series, AR160 series, AR200 series, AR1200 series, AR2200 (except AR2204XE, AR2204XE-DC, AR2240C): 0 to 15 • AR2204XE, AR2204XE-DC, AR2240C, AR3600 series: 0 to 31 • AR3200 series: 0 to 7

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 **19.6.5 acl-id (user group view)**). 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.

Precautions

- The device supports a maximum of 32 user groups.
- 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.

 Copyright © Huawei Technologies Co., Ltd.

- If you want to delete the user group when the ACL bound to the user takes effect, run the **cut access-user user-group** command to disconnect all users bound to the user group.
- 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 also cannot be 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 groups A and B both cannot take effect. To make the user group authorization information delivered by the authentication server take effect, ensure that this user group is configured on the device. To make the user group authorization information applied in the AAA domain take effect, ensure that the authentication server does not deliver any user group attribute.

Example

Create a user group **test1**.

```
<Huawei> system-view
[Huawei] user-group test1
```

19.6.151 user-isolated

Function

The **user-isolated** command configures inter-group or intra-group isolation in a user group.

The **undo user-isolated** command disables inter-group or intra-group isolation in a user group.

By default, inter-group or intra-group isolation is not configured in a user group.

Format

user-isolated { **inter-group** | **inner-group** } *

undo user-isolated { **inter-group** | **inner-group** } *

Parameters

Item	Description	Value
inter-group	Configures inter-group isolation.	-
inner-group	Configures intra-group isolation.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After inter-group isolation is configured in a user group, users in the user group cannot communicate with users in other user groups.

After intra-group isolation is configured in a user group, users in the user group cannot exchange Layer 2 or Layer 3 packets with each other.

Precautions

After authorized users go online, the RADIUS server dynamically delivers user group information. In this situation, the inter-group or intra-group isolation configuration cannot be modified or deleted.

Example

Configure intra-group isolation in user group **general-group**.

```
<Huawei> system-view
[Huawei] user-group general-group
[Huawei-user-group-general-group] user-isolated inter-group inner-group
```

19.6.152 user-vlan

Function

The **user-vlan** command binds a VLAN to a user group.

The **undo user-vlan** command unbinds a VLAN from a user group.

By default, no VLAN is bound to a user group.

Format

user-vlan *vlan-id*

undo user-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN bound to a user group.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a user group using the **user-group** command, you can run the **user-vlan** command to bind a VLAN to the user group. The device will deliver the authorization VLAN based on the user group. When a user in the user group goes online, the user will be added to the VLAN and obtain network access rights of the user group.

Prerequisites

- The VLAN to be bound to a user group has been created using the **6.3.43 vlan** command.

Precautions

- An authorized VLAN cannot be delivered to online Portal users.
- This command does not take effect for users who are already online.

Example

Configure VLAN 10 as the authorization VLAN for the user group **abc**.

```
<Huawei> system-view
[Huawei] vlan batch 10
[Huawei] user-group abc
[Huawei-user-group-abc] user-vlan 10
```

Related Topics

19.6.51 display user-group

19.6.153 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*

 Copyright © Huawei Technologies Co., Ltd.

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 on the device.

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
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.154 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 UDP 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] web-auth-server listening-port 3000
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.155 web-auth-server (Portal access profile view)

Function

The **web-auth-server** command configures the Portal server profile 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 profile.

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 profile.	The value must be an existing Portal server profile name.
bak-server-name	Specifies the name of a backup Portal server profile. **NOTE** The name of the backup Portal server profile cannot be configured to the command-line keywords **direct** and **layer3**.	The value must be an existing Portal server profile 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

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After a Portal server profile 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 profile 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 **19.6.135 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 IP address and MAC address.
- **layer3**: When there is a Layer 3 forwarding device between the device and a user, 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 profile has been created using **19.6.157 web-auth-server (system view)** and the IP address of the Portal server has been configured using **19.6.136 server-ip (Portal server profile view)**.

Precautions

- After a Portal access profile is bound to an authentication profile, the Portal server profile used in the Portal access profile cannot be deleted, but can be modified.
- This command does not take effect on the VLANIF interface corresponding to the super VLAN.

Example

Bind the Portal access profile **p1** to the Portal server profiles **server1** and **server2** (backup Portal server profile), 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-acces-profile-p1] web-auth-server server1 server2 direct
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.6.157 web-auth-server (system view)
19.6.136 server-ip (Portal server profile view)
19.6.52 display web-auth-server configuration
19.6.31 display authentication-profile configuration

19.6.156 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable the device from transparently transmitting users' authentication responses to the Portal server.

```
<Huawei> system-view
[Huawei] undo web-auth-server reply-message
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.157 web-auth-server (system view)

Function

The **web-auth-server** command creates a portal server profile or displays the portal server profile view.

The **undo web-auth-server** command deletes a portal server profile.

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, or the first character or several leftmost characters of these character strings.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

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 profile 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 profile:

- Run the **19.6.136 server-ip (Portal server profile view)** command to configure an IP address for the portal server.
- Run the **19.6.143 url (Portal server profile view)** command to configure a URL of the portal server.
- Run the **19.6.98 port (Portal server profile view)** command to set the port number that a portal server uses to receive notification packets from the device.
- Run the **19.6.137 shared-key (Portal server profile view)** 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.

A maximum of eight portal server profiles can be configured on the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create portal server profile named **huawei**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
```

Related Topics

19.6.52 display web-auth-server configuration
19.6.143 url (Portal server profile view)
19.6.136 server-ip (Portal server profile view)
19.6.98 port (Portal server profile view)
19.6.137 shared-key (Portal server profile view)

19.6.158 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

 Copyright © Huawei Technologies Co., Ltd.

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
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.159 web-redirection disable (Portal server profile 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 profile 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable the Portal authentication redirection function.

```
<Huawei> system-view
[Huawei] web-auth-server nac
[Huawei-web-auth-server-nac] web-redirection disable
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.160 web-service aaa server

Function

The **web-service aaa server** command configures a URL for the authentication and accounting server and enables the function of receiving user authorization information.

The **undo web-service aaa server** command deletes the URL configured for the authentication and accounting server and disables the function of receiving user authorization information.

By default, no URL is configured for the authentication and accounting server, and the function of receiving user authorization information is disabled.

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW that can work as a WLAN Fat AP support this command.

Format

web-service aaa server *url* **authorize-enable**

undo web-service aaa server

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url	Specifies the URL of the authentication and accounting server.	The value is a string of 1 to 128 characters in the format of **[http://]host[:port]**. • host: indicates an IP address or a domain name. • port: indicates a port number. The default value is 80. You need to add the port number to the IP address or domain name only when the default port number is changed. **NOTE** If the value of **host** is in the domain name format, configure a DNS table before using this command; otherwise, the IP address matching the domain name cannot be obtained. If the DNS table is modified after this command is executed, run this command again.
authorize-enable	The function of receiving user authorization information is enabled.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Users connecting to the device through Wi-Fi can access the Internet only after being authenticated by the authentication and accounting server. You can run this command to configure a URL for the authentication and accounting server, and enable the function of receiving user authorization information. User authorization information includes online duration, traffic usage, and user bandwidth. When a user accesses the Internet, the device periodically sends accounting packets to the

 Copyright © Huawei Technologies Co., Ltd.

authentication and accounting server. The server performs accounting for the users based on user traffic statistics. When the online duration or traffic usage exceeds authorization, the device forcibly disconnects the user and sends the disconnection message of the user to the authentication and accounting server.

Example

Configure a URL for the authentication and accounting server and enable the function of receiving user authorization information.

```
<Huawei> system-view
[Huawei] web-service aaa server http://10.1.1.1:81 authorize-enable
```

19.6.161 web-service access enable

Function

The **web-service access enable** command enables authentication and accounting functions on a WLAN-BSS interface.

The **undo web-service access enable** command disables authentication and accounting functions on a WLAN-BSS interface.

By default, authentication and accounting functions are disabled on a WLAN-BSS interface.

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW that can work as a WLAN Fat AP support this command.

Format

web-service access enable

undo web-service access enable

Parameters

None

Views

WLAN-BSS interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Users connecting to the device through Wi-Fi can access the Internet only after being authenticated. After authentication and accounting functions are enabled on a WLAN-BSS interface using this command, the device provides authentication and accounting functions to users.

Example

Enable authentication and accounting functions on a WLAN-BSS interface.

```
<Huawei> system-view
[Huawei] interface wlan-bss 0

[Huawei-Wlan-Bss0] web-service access enable
```

19.6.162 web-service accounting enable

Function

The **web-service accounting enable** command enables the device to send accounting packets to the authentication and accounting server.

The **undo web-service accounting enable** command disables the device from sending accounting packets to the authentication and accounting server.

By default, the device does not send accounting packets to the authentication and accounting server.

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW that can work as a WLAN Fat AP support this command.

Format

web-service accounting enable

undo web-service accounting enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

After a user connects to the device through Wi-Fi, is authenticated by the authentication and accounting server, and obtains rights, the user can access the websites outside the whitelist. This command enables the device to send accounting request packets to the authentication and accounting server. When the authorized online traffic volume and duration of an online user are not exceeded, the device periodically sends accounting packets to the authentication and accounting server. The server performs accounting on the user based on the traffic usage when the user stays online.

Example

Enable the device to send accounting packets to the authentication and accounting server.

```
<Huawei> system-view
[Huawei] web-service accounting enable
```

Related Topics

19.6.163 web-service accounting interval

19.6.163 web-service accounting interval

Function

The **web-service accounting interval** command configures the interval at which the device sends accounting packets to the authentication and accounting server.

The **undo web-service accounting interval** command restores the default interval at which the device sends accounting packets to the authentication and accounting server.

By default, the device sends accounting packets to the authentication and accounting server at an interval of 30 seconds.

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW that can work as a WLAN Fat AP support this command.

Format

web-service accounting interval *interval*

undo web-service accounting interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the device sends accounting packets to the authentication and accounting server.	The value is an integer that ranges from 5 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Users connecting to the device through Wi-Fi can access the Internet only after being authenticated by the authentication and accounting server. You can run this command to configure the interval at which the device sends accounting packets to the authentication and accounting server.

Example

Set the interval at which the device sends accounting packets to the authentication and accounting server to 10 seconds.

```
<Huawei> system-view
[Huawei] web-service accounting interval 10
```

19.7 ACL Configuration Commands

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support the ACL configured for Layer 2 forwarding traffic.

19.7.1 acl ipv6 name

Function

The **acl ipv6 name** command creates a named ACL6 and enters the ACL6 view.

The **undo acl ipv6 name** command deletes a named ACL6.

By default, no named ACL6 is created.

 Copyright © Huawei Technologies Co., Ltd.

Format

acl ipv6 name *acl6-name* [**advance** | **basic** | *acl6-number*] [**match-order** { **auto** | **config** }]

undo acl ipv6 name *acl6-name*

Parameters

Parameter	Description	Value
acl6-name	Specifies the name of an ACL6.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
advance	Indicates an advanced ACL6.	-
basic	Indicates a basic ACL6.	-
acl6-number	Specifies the number of an ACL6.	The value is an integer that ranges from 2000 to 3999. ● The value of a basic ACL6 ranges from 2000 to 2999. ● The value of an advanced ACL6 ranges from 3000 to 3999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL6 rules. • **auto**: indicates that ACL6 rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. • **config**: indicates that ACL6 rules are matched based on the configuration order. The ACL6 rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL6 rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL6 is a set of rules composed of **permit** or **deny** clauses. ACL6s are mainly used in QoS. ACL6s can limit data flows to improve network performance. For example, ACL6s are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Run the **rule** command to configure ACL6 rules and apply the ACL6 to services which packets need to be filtered.

Precautions

If the number of a named ACL6 is not specified, the Router allocates a number to the named ACL6. The following situations are involved:

- If only the type of a named ACL6 is specified, the number of the named ACL6 allocated by the Router is the maximum value of the named ACL6 of the type.
- If the number and the type of a named ACL6 are not specified, the Router considers the named ACL6 as the advanced ACL6 and allocates the maximum value to the named ACL6.

After you create a named ACL6 by using the **acl ipv6 name** command, the ACL6 still exists even if you exit from the ACL6 view. You must run the **undo acl ipv6 name** *acl6-name* or **undo acl ipv6** *acl6-number* command to delete the ACL6.

When you delete an ACL6 that has been referenced by other services, the services may be interrupted. Therefore, before deleting an ACL6, ensure that the ACL6 is not in use.

Example

Create basic ACL6 2001 named **test2**.

```
<Huawei> system-view
[Huawei] acl ipv6 name test2 2001
```

Related Topics

19.7.8 display acl ipv6

19.7.2 acl ipv6 (system view)

Function

The **acl ipv6** command creates a numbered ACL6 and enters the ACL6 view.

The **undo acl ipv6** command deletes a numbered ACL6.

By default, no numbered ACL6 is created.

Format

acl ipv6 [**number**] *acl6-number* [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | [**number**] *acl6-number* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Indicates the number that identifies an ACL.	-
acl6-number	Specifies an ACL6 number.	The value is an integer that ranges from 2000 to 3999. • The value of a basic ACL6 ranges from 2000 to 2999. • The value of an advanced ACL6 ranges from 3000 to 3999.
match-order { **auto** | **config** }	Indicates the matching order of ACL6 rules. • **auto**: indicates that ACL6 rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. • **config**: indicates that ACL6 rules are matched based on the configuration order. The ACL6 rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL6 rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used.	-
all	Indicates that all the configured ACL6s are deleted.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

An ACL6 is a set of rules composed of **permit** or **deny** clauses. ACL6 rules can be referenced by modules. ACL6s are applicable to QoS. ACL6s can limit data flows to improve network performance. For example, ACL6s are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.

Follow-up Procedure

Run the **rule** command to configure ACL6 rules and apply the ACL6 to services which packets need to be filtered.

Precautions

After you create a named ACL6 by using the **acl ipv6** command, the ACL6 still exists even if you exit from the ACL6 view. You must run the **undo acl ipv6** *acl6-number* command to delete the ACL6.

When you delete an ACL6 that has been referenced by other services, the services may be interrupted. Before deleting an ACL6, ensure that the ACL6 is unused.

All ACL6s can be deleted on the device at one time, whereas this method is not recommended.

Example

Create an ACL6 with the number of 3000.

```
<Huawei> system-view
[Huawei] acl ipv6 number 3000
```

Related Topics

19.7.8 display acl ipv6

19.7.19 rule (basic ACL6 view)

19.7.17 rule (advanced ACL6 view)

19.7.3 acl name

Function

The **acl name** command creates a named ACL and enters the ACL view.

The **undo acl** command deletes a named ACL.

By default, no ACL is created.

Format

acl name *acl-name* [**advance** | **basic** | **link** | *acl-number*] [**match-order** { **auto** | **config** }]

undo acl name *acl-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-name	Specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
advance	Indicates an advanced ACL.	-
basic	Indicates a basic ACL.	-
link	Indicates a Layer 2 ACL.	-
acl-number	Specifies the number of an ACL.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL rules. • **auto**: indicates that ACL rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. • **config**: indicates that ACL rules are matched based on the configuration order. The ACL rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL consists of a series of rules defined by multiple **permit** or **deny** clauses. ACLs are mainly applied to QoS, route filtering, and user access. The major functions of ACLs are as follows:

 Copyright © Huawei Technologies Co., Ltd.

- Limit data flows to improve network performance. For example, ACLs are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.
- Provide flow control. For example, ACLs are used to limit transmission of routing updates so that the bandwidth is saved.
- Provide network access security. For example, ACLs are configured to allow specified users to access the human resource network.

Follow-up Procedure

Run the **rule** command to configure ACL rules and apply the ACL to services which packets need to be filtered.

Precautions

After you create a named ACL by using the **acl name** command, the ACL still exists even if you exit from the ACL view. You must run the **undo acl name** *acl-name* or **undo acl** *acl-number* command to delete the ACL.

When you delete an ACL that has been referenced by other services, the services may be interrupted. Before deleting an ACL, ensure that the ACL is not in use.

If the number of a named ACL is not specified, the device automatically allocates a number to the named ACL. The following situations are involved:

- If the type of a named ACL is specified, the number of the named ACL allocated by the device is the maximum value of the named ACL of the type.
- If the number and the type of a named ACL are not specified, the device considers the named ACL as the advanced ACL and allocates the maximum value to the named ACL.

The Router does not allocate the number to a named ACL repeatedly.

Example

Create basic ACL 2001 named **test1**.

```
<Huawei> system-view
[Huawei] acl name test1 2001
```

Related Topics

19.7.7 display acl

19.7.4 acl (system view)

Function

The **acl** command creates an ACL with the specified number and enters the ACL view.

The **undo acl** command deletes a specified ACL.

By default, no ACL is created.

 Copyright © Huawei Technologies Co., Ltd.

Format

acl [**number**] *acl-number* [**match-order** { **auto** | **config** }]

undo acl { [**number**] *acl-number* | **all** }

Parameters

Parameter	Description	Value
number	Specifies the number that identifies an ACL.	-
acl-number	Specifies the number of an ACL.	The value is an integer. • The number of a basic ACL ranges from 2000 to 2999. • The number of an advanced ACL ranges from 3000 to 3999. • The number of a Layer 2 ACL ranges from 4000 to 4999. • The number of a user ACL ranges from 6000 to 6031.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL rules. • **auto**: indicates that ACL rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. • **config**: indicates that ACL rules are matched based on the configuration order. The ACL rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used.	-
all	Indicates that all ACLs are deleted.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL consists of a series of rules defined by multiple **permit** or **deny** clauses. ACLs are mainly applied to QoS, route filtering, and user access. The major functions of ACLs are as follows:

 Copyright © Huawei Technologies Co., Ltd.

- Limit data flows to improve network performance. For example, ACLs are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.
- Provide flow control. For example, ACLs are used to limit transmission of routing updates so that the bandwidth is saved.
- Provide network access security. For example, ACLs are configured to allow specified users to access the human resource network.

Follow-up Procedure

Run the **rule** command to configure ACL rules and apply the ACL to services which packets need to be filtered.

Precautions

After you create an ACL by using the **acl** command, the ACL still exists even if you exit from the ACL view. You must run the **undo acl** *acl-number* command to delete the ACL.

When you delete an ACL that has been referenced by other services, the services may be interrupted. Before deleting an ACL, ensure that the ACL is not in use.

You are advised not to delete all ACLs because this operation may cause a service interruption.

Example

Create an ACL numbered 2000.

```
<Huawei> system-view
[Huawei] acl number 2000
```

Related Topics

19.7.7 display acl
19.7.18 rule (basic ACL view)
19.7.16 rule (advanced ACL view)
19.7.20 rule (layer 2 ACL view)
19.7.21 rule (user ACL view)

19.7.5 acl logging

Function

The **acl logging** command sets the update interval and aging timeout for the simplified ACL log.

By default, the update interval and aging timeout of the simplified ACL log are 900 seconds.

Format

acl logging { **timeout** | **update** } { *interval* | **default** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
timeout	Indicates the aging timeout of the simplified ACL log.	-
update	Indicates the update interval of the simplified ACL log.	-
interval	Specifies the value of update interval or aging timeout.	The value is an integer that ranges from 30 to 65535, in seconds.
default	Restores the default update interval or aging timeout.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After simplified ACL is configured, the device periodically (300 seconds earlier or later than the update interval) prints the simplified ACL log entries that have not been aged out. You can check information about the packets matching the simplified ACL. You can use this command to set the update interval and aging timeout of the simplified ACL log.

The display mode of ACL logs is recorded in the **QOS/4/SACL_LOG** log.

Example

Set the update interval of the simplified ACL log to 300 seconds.

```
<Huawei> system-view
[Huawei] acl logging update 300
```

19.7.6 description

Function

The **description** command configures the description of an ACL.

The **undo description** command deletes the description of an ACL.

By default, no description is configured for an ACL.

 Copyright © Huawei Technologies Co., Ltd.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Describes an ACL.	The value is a string of 1 to 127 case-sensitive characters with spaces supported.

Views

ACL view, ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the description of an ACL, for example, the usage or application scenario of the ACL. It is used to differentiate ACLs.

Prerequisites

The ACL to be described has been created.

Configuration Impact

If you run the **description** command multiple times in the same ACL view, only the latest configuration takes effect.

Example

Configure the description of ACL 2100.

```
<Huawei> system-view
[Huawei] acl 2100
[Huawei-acl-basic-2100] description This acl is used in QoS policy
[Huawei-acl-basic-2100] display acl 2100
Basic ACL 2100, 0 rule
This acl is used in QoS policy
ACL's step is 5
```

Configure the description of ACL6 2100.

```
<Huawei> system-view
[Huawei] acl ipv6 2100
[Huawei-acl6-basic-2000] description This acl6 is used in QoS policy
[Huawei-acl6-basic-2100] display acl ipv6 2100
```

 Copyright © Huawei Technologies Co., Ltd.

```
Basic IPv6 ACL 2100, 0 rule
This acl6 is used in QoS policy
Acl's step is 5
```

Related Topics

19.7.4 acl (system view)

19.7.3 acl name

19.7.2 acl ipv6 (system view)

19.7.7 display acl

Function

The **display acl** command displays the configuration of an ACL.

Format

display acl { *acl-number* | **name** *acl-name* | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer. • The number of a basic ACL ranges from 2000 to 2999. • The number of a numbered advanced ACL ranges from 3000 to 3999. • The number of a Layer 2 ACL ranges from 4000 to 4999. • The number of a user ACL ranges from 6000 to 6031.
name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
all	Indicates all ACLs.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **display acl** command displays the ACL configuration.

Configuration Impact

The **display acl** command takes effect only for the MQC service.

Example

Display configuration about the ACL named **test**.

```
<Huawei> display acl name test
Advanced ACL test 3999, 1 rule, match-order is auto
Acl's step is 5
 rule 5 permit ip destination 10.10.10.1 0 (2 matches)
```

Display the ACL configuration.

```
<Huawei> display acl all
 Total quantity of nonempty ACL number is 1

Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 permit ip dscp cs1 (2 matches)
```

Table 19-70 Description of the **display acl** command output

Item	Description
Advanced ACL test 3999, 1 rule, match-order is auto	Advanced ACL 3999 named **test** that matches in the automatic order and contains one rule.
Acl's step is 5	The ACL's step is 5. To set the step between ACL rule IDs, run the **step** command.
rule 5 permit ip destination 10.10.10.1 0 (2 matches)	Rule 5 that matches packets whose source IP address is 10.10.10.1. The number of packets that match Rule 5 is 2. If no packet is matched, the **matches** field is not displayed. To modify an advanced ACL rule, run the **rule (advanced ACL view)** command.
Total quantity of nonempty ACL number is 1	One ACL contains rules.
Advanced ACL 3000, 1 rule	Advanced ACL 3000 contains one rule.
rule 5 permit ip dscp cs1 (2 matches)	Rule 5 that matches packets with DSCP priorities. The number of packets that match Rule 5 is 2. To modify an advanced ACL rule, run the **rule (advanced ACL view)** command.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.7.4 acl (system view)
19.7.6 description
19.7.18 rule (basic ACL view)
19.7.16 rule (advanced ACL view)
19.7.20 rule (layer 2 ACL view)
19.7.21 rule (user ACL view)
19.7.23 step

19.7.8 display acl ipv6

Function

The **display acl ipv6** command displays the configuration of a specific ACL6 or all ACL6s.

Format

display acl ipv6 { *acl6-number* | **name** *acl6-name* | **all** }

Parameters

Parameter	Description	Value
acl6-number	Specifies an ACL6 number.	The value is an integer that ranges from 2000 to 3999. The ACL6 with a number ranging from 2000 to 2999 is a basic ACL6 and the ACL6 with a number ranging from 3000 to 3999 is an advanced ACL6.
name *acl6-name*	Displays the ACL6 with a specified name.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
all	Displays the configurations of all ACL6s.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display acl ipv6** command displays the ACL6 configuration.

Example

Display the configuration about the ACL6 with the number of 2000.

```
<Huawei> display acl ipv6 2000

Basic IPv6 ACL 2000, 2 rules
Acl's step is 5
 rule 5 deny source 3::/64
 rule 10 permit source 4::/64
```

Display the ACL6 configuration.

```
<Huawei> display acl ipv6 all
 Total nonempty acl6 number is 1

Basic IPv6 ACL 2000, 2 rules
Acl's step is 5
 rule 5 deny source 3::/64
 rule 10 permit source 4::/64 (2 matches)
```

Table 19-71 Description of the display acl ipv6 command output

Item	Description
Total nonempty acl6 number is 1	One ACL6 contains rules.
Basic IPv6 ACL 2000, 2 rules	ACL6 2000, which is a basic ACL6 and has two rules.
Acl's step is 5	ACL's step is 5. To set the step between ACL rule IDs, run the **step** command.
rule 5 deny source 3::/64	ACL6 rule 5, which denies packets with the source IPv6 address 3::/64. To modify a basic ACL6 rule, run the **rule (rule basic acl6 view)** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
rule 10 permit source 4::/64 (2 matches)	ACL6 rule 10, which permits packets with the source IPv6 address 4::/64. The number of packets that match Rule 10 is 2. If no packet is matched, the **matches** field is not displayed. To modify a basic ACL6 rule, run the **rule (rule basic acl6 view)** command.

Related Topics

19.7.2 acl ipv6 (system view)
19.7.19 rule (basic ACL6 view)
19.7.17 rule (advanced ACL6 view)
19.7.23 step

19.7.9 display acl resource

Function

The **display acl resource** command displays information about ACL resources.

Format

display acl resource [**slot** *slot-id*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
slot *slot-id*	Displays ACL rules on the specified LPU. *slot-id* specifies the slot ID of the LPU. • If the **slot** parameter is not specified, the ACL resources on the SRU are displayed. • If the **slot** parameter is specified: – When the LAN-side interface card 8FE1GE or 24GE is in the slot specified by *slot-id*, the ACL rules on the Ethernet LAN interface card are displayed. – When a WAN-side card or a LAN-side card of another type is in the slot specified by *slot-id*, the ACL resources on the main control board are displayed.	Set the value according to the device configuration. **NOTE** AR100&AR120&AR150&AR160&AR200 do not support this parameter.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If ACL configuration fails, all the ACL resources on the device may have been used up. You can run the **display acl resource** command to check whether there are available ACL resources (including ACL4 and ACL6).

Example

View ACL rules on the SRU.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display acl resource
 Slot: 0
-------------------------------------------------------------------------
 Type              Total    Reserved    Remaining  Configured
-------------------------------------------------------------------------
 ACL                8192      N/A         6904       1288
 Meter              8192      N/A         8189       3
 Counter            8192      N/A         8188       4
-------------------------------------------------------------------------
```

Table 19-72 Description of the display acl resource command output

Item	Description
Slot: 0	The slot ID of the board is 0.
Type	Resource type. • ACL: all ACL rules. • Meter: ACL rules applied to the traffic classifier that is bound to the traffic policing action. • Counter: ACL rules applied to the traffic classifier.
Total	Total number of ACL rules of the specified type.
Reserved	Number of reserved ACL rules of the specified type.
Remaining	Number of remaining ACL rules of the specified type.
Configured	Number of configured ACL rules of the specified type.

Related Topics

19.7.4 acl (system view)

19.7.10 display time-range

Function

The **display time-range** command displays the configuration and status of the current time range.

Format

display time-range { **all** | *time-name* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
all	Indicates all the configured time ranges.	-
time-name	Specifies the name of a time range during which ACL rules take effect.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To specify a time range during which ACL rules take effect, run the **time-range** command to configure the time range and reference the time range name when you configure an ACL.

Before using a time range to filter data packets, run the **display time-range** command to view the time range configuration to avoid duplicate time ranges.

NOTE

The device updates the status of ACLs with a delay of about 10 seconds. The **display time-range** command adopts the current time range to determine the status of ACLs; therefore, you may find that the ACL using an active time range is inactive. This is normal.

Example

Display the configuration and status of all time ranges.

```
<Huawei> display time-range all
Current time is 14:48:13 10-17-2012 Wednesday

Time-range : abc (Active)
from 23:23 2012/9/9 to 23:59 2012/12/31
```

Table 19-73 Description of the display time-range command output

Item	Description
Current time is 14:48:13 10-17-2012 Wednesday	The current time is Wednesday 14:48:13 10-17-2012.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Time-range:abc (Active)	The time range is named **abc** and is active. The time range can be: • Active. • Inactive.
from 23:23 2012/9/9 to 23:59 2012/12/31	Time range abc is from 23:23 2012/9/9 to 23:59 2012/12/31.

Related Topics

19.7.24 time-range

19.7.11 ip port-set

Function

The **ip port-set** command creates a port set and displays the port set view.

The **undo ip port-set** command deletes a port set.

By default, no port set is created.

Format

ip port-set *port-set-name* **protocol** { **tcp** | **udp** }

undo ip port-set *port-set-name*

Parameters

Parameter	Description	Value
port-set-name	Specifies the port set name.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter, spaces not supported.
protocol { **tcp**	**udp** }	Specifies the protocol type, TCP or UDP.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If an advanced ACL rule matching source or destination port numbers is complex or the same port rules need to be defined for multiple ACL rules, you can configure a port set and bind the port set to the advanced ACL.

Follow-up Procedure

Run the **19.7.12 port (port set view)** command to create port rules for the port set and bind the port set to the advanced ACL.

Precautions

- A port set without port rules cannot be bound to an advanced ACL.
- The protocol type specified in the port set must be the same as the protocol type specified in the advanced ACL.

Example

Create the port set **fromCenter** with the protocol type TCP, configure rules for ACL 3000, and bind the port set **fromCenter** to ACL 3000.

```
<Huawei> system-view
[Huawei] ip port-set fromCenter protocol tcp
[Huawei-port-set-fromCenter] port range 1000 2000
[Huawei-port-set-fromCenter] quit
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule permit tcp destination-port port-set fromCenter
```

Related Topics

19.7.12 port (port set view)

19.7.16 rule (advanced ACL view)

19.7.12 port (port set view)

Function

The **port** command configures port rules for a port set.

The **undo port** command deletes port rules of a port set.

By default, no port rule is configured.

Format

port [*port-rule-id*] { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }

undo port *port-rule-id*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
port-rule-id	Specifies the port rule ID. • If the rule matching the specified ID already exists, the new rule will overwrite the old rule. If no rule matches the specified ID, a rule is created, and inserted into the rule list based on the ID order. • If a rule is created without specifying its ID, an ID following the existing IDs is automatically allocated to the rule.	The value is an integer that ranges from 0 to 63.
eq *port*	Indicates the port number equivalent to the specified value.	The port number may be a name or numeral. If the port number is a numeral, the value ranges from 0 to 65535.
gt *port*	Indicates the port numbers greater than the specified value.	
lt *port*	Indicates the port numbers smaller than the specified value.	
range *port-start port-end*	Indicates a port number range. *port-start* indicates the start port number, and *port-end* indicates the end port number.	

Views

Port set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

When configuring an advanced ACL, you can bind a port set with port rules configured to the advanced ACL, specifying the source or destination port number for the ACL rules.

Prerequisites

The **ip port-set** command has been run to create a port set.

Example

Set the port range to 1000-2000.

```
<Huawei> system-view
[Huawei] ip port-set fromCenter protocol tcp
[Huawei-port-set-fromCenter] port 0 range 1000 2000
```

Related Topics

19.7.11 ip port-set

19.7.13 reset acl counter

Function

The **reset acl counter** command clears statistics about ACLs.

Format

reset acl counter { **name** *acl-name* | *acl-number* | **all** }

Parameters

Parameter	Description	Value
name *acl-name*	Specifies the name of an ACL whose statistics need to be cleared.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
acl-number	Specifies the number of an ACL whose statistics need to be cleared.	The value is an integer. • The number of a basic ACL ranges from 2000 to 2999. • The number of a numbered advanced ACL ranges from 3000 to 3999. • The number of a Layer 2 ACL ranges from 4000 to 4999.
all	Clears all the ACL statistics.	-

Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain the accurate ACL statistics generated in a certain period, run the **reset acl counter** command to clear existing statistics and start statistics collection.

NOTICE

After the **reset acl counter** command is executed, the system does not prompt you the statistics deletion.

Before using the **reset acl counter** command, determine whether you intend to clear ACL statistics.

Follow-up Procedure

After running the **reset acl counter** command to clear the previous ACL statistics, you can use the **display acl** command to view ACL rules and statistics on the packets matching the ACL rules in the current period.

Example

Clear statistics about ACL 2000.

```
<Huawei> reset acl counter 2000
```

Related Topics

19.7.7 display acl

19.7.14 reset acl ipv6 counter

Function

The **reset acl ipv6 counter** command clears the ACL6 statistics.

Format

reset acl ipv6 counter { **name** *acl6-name* | *acl6-number* | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name *acl6-name*	Specifies the name of an ACL6 whose statistics need to be cleared.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
acl6-number	Specifies the number of an ACL6 whose statistics need to be cleared.	The value is an integer that ranges from 2000 to 3999. • ACL6s numbered 2000 to 2999 are basic ACL6s. • ACL6s numbered 3000 to 3999 are advanced ACL6s.
all	Clears all the ACL6 statistics.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain the accurate ACL6 statistics in a certain period, run the **reset acl ipv6 counter** command to clear existing statistics and start statistics collection.

NOTICE

Before using the **reset acl ipv6 counter** command, determine whether you intend to clear ACL6 statistics.

After the **reset acl ipv6 counter** command is executed, the system does not prompt you the statistics deletion.

Follow-up Procedure

After running the **reset acl ipv6 counter** command to clear the previous ACL statistics, you can use the **display acl ipv6** command to view ACL rules and statistics on the packets matching the ACL rules in the current period.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear the statistics about basic ACL6 2000.

```
<Huawei> reset acl ipv6 counter 2000
```

Related Topics

19.7.8 display acl ipv6

19.7.15 reset acl logging

Function

The **reset acl logging** command deletes all simplified ACL logs.

Format

reset acl logging

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

When there are simplified ACL logs that have not been aged out on the device, the device prints these logs at the specified interval. This command can clear all simplified ACL logs on the device, except the printed ones.

Example

Delete all simplified ACL logs on the device.

```
<Huawei> reset acl logging
```

19.7.16 rule (advanced ACL view)

Function

The **rule** command adds or modifies an advanced ACL rule.

The **undo rule** command deletes an advanced ACL rule.

By default, no advanced ACL rule is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

- When the Internet Control Management Protocol (ICMP) is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- When the Transmission Control Protocol (TCP) is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** | **established** } * | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- When the User Datagram Protocol (UDP) is used, run:

  rule [*rule-id*] { **deny** | **permit** }{ *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- When GRE, IGMP, IPinIP, or OSPF is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- When the IP protocol version is IPv4, run:

  rule [*rule-id*] { **deny** | **permit** } **ip** [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- To delete an advanced ACL rule, run:

  undo rule *rule-id* [**destination** | **destination-port** | **icmp-type** | **source** | **source-port** | **tcp-flag** | **logging** | **time-range** | **vpn-instance** | [**dscp** | [**tos** | **precedence**] *] | [**fragment** | **none-first-fragment**]] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. • If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. • If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically start from the step value. The default step is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
icmp	Indicates that the protocol type is ICMP. The value 1 indicates that ICMP is specified.	-
tcp	Indicates that the protocol type is TCP. The value 6 indicates that TCP is specified.	-
udp	Indicates that the protocol type is UDP. The value 17 indicates that UDP is specified.	-
protocol-number	Indicates the protocol type expressed by name or number. **NOTE** Parameters in an ACL vary with the protocol type. The combination of **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } and **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } is applicable to TCP and UDP only.	The value expressed by number is an integer that ranges from 1 to 255. The value expressed by name can be **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **ospf**, **tcp**, or **udp**. **icmp**, **tcp**, **udp**, **gre**, **igmp**, **ipinip**, and **ospf** correspond to 1, 6, 17, 47, 2, 4, and 89.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination { *destination-address destination-wildcard* | **any** }	Indicates the destination IP address of packets that match ACL rules. If this parameter is not specified, packets with any destination IP address are matched. • *destination-address*: specifies the destination IP address of data packets. • *destination-wildcard*: specifies the wildcard mask of the destination IP address. • **any**: indicates any destination IP address of packets. That is, the value of *destination-address* is 0.0.0.0 or the value of *destination-wildcard* is 255.255.255.255.	*destination-address*: The value is in dotted decimal notation. *destination-wildcard*: The value is in dotted decimal notation. The wildcard mask of the destination IP address can be 0, equivalent to 0.0.0.0, indicating that the destination IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.
icmp-type { *icmp-name* | *icmp-type icmp-code* }	Indicates the type and code of ICMP packets, which are valid only when the protocol of packets is ICMP. If this parameter is not specified, all types of ICMP packets are matched. • *icmp-name*: specifies the name of ICMP packets. • *icmp-type*: specifies the type of ICMP packets. • *icmp-code*: specifies the code of ICMP packets.	*icmp-type* is an integer that ranges from 0 to 255. *icmp-code* is an integer that ranges from 0 to 255. **Table 19-75** lists the mapping between ICMP names and ICMP types and codes.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source { *source-address* *source-wildcard* | **any** }	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. • *source-address*: specifies the source IP address of packets. • *source-wildcard*: specifies the wildcard mask of the source IP address. • **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 or the value of *source-wildcard* is 255.255.255.255.	*source-address* : The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ack (010000).	-
fin	Indicates that the SYN Flag type in the TCP packet header is fin (000001).	-
psh	Indicates that the SYN Flag type in the TCP packet header is psh (001000).	-
rst	Indicates that the SYN Flag type in the TCP packet header is rst (000100).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
syn	Indicates that the SYN Flag type in the TCP packet header is syn (000010).	-
urg	Indicates that the SYN Flag type in the TCP packet header is urg (100000).	-
established	Indicates that the SYN Flag type in the TCP packet header is ack(010000) or rst(000100).	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: • **eq** *port*: equivalent to the destination port number. • **gt** *port*: greater than the destination port number. • **1t** *port*: smaller than the destination port number. • **range** *port-start port-end*: destination port number range. *port-start* specifies the start port number. *port-end* specifies the end port number. • **port-set** *port-set-name*: binds a port set to specify destination ports.	• The value of *port* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. • The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535. • *port-set-name* is the name of an existing port set.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: • **eq** *port*: equivalent to the source port number. • **gt** *port*: greater than the source port number. • **1t** *port*: smaller than the source port number. • **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number. • **port-set** *port-set-name*: binds a port set to specify source ports.	• The value of *port* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. • The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535. • *port-set-name* is the name of an existing port set.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** The ACL with the **vpn-instance** *vpn-instance-name* parameter specified is only applied to firewall and IPSec features.	The value is a string of 1 to 31 characters without spaces. Letters, digits, underscores (_), and dots (.) are allowed.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dscp *dscp*	Specifies the value of a Differentiated Services Code Point (DSCP). **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value is an integer or a name. • The value ranges from 0 to 63 when it is an integer. • When it is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. • The value ranges from 0 to 15 when it is an integer. • When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 19-74** describes the mapping between ToS names and values.
precedence *precedence*	Indicates that packets are filtered based on the precedence field. *precedence* specifies the precedence value.	The value ranges from 0 to 7. The values 0 to 7 correspond to *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network*.
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
none-first-fragment	Indicates that the rule is valid for only non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments. **NOTE** The rules that do not contain fragment or none-first-fragment parameters are valid for all packets.	-
vni *vni-id*	Specifies the VNI ID of the packets that match the rule. **NOTE** This parameter is valid only in the VXLAN scenario.	The value is an integer that ranges from 0 to 16777215.
logging	Specifies the log recording the IP information, port number, and protocol type of the packets that match the rule. **NOTE** The **logging** only takes effect when the **traffic-filter** command references ACLs.	-

Table 19-74 Mapping between ToS names and values

ToS Name	Value	ToS Name	Value
normal	0	max-reliability	2
min-monetary-cost	1	max-throughput	4
min-delay	8	-	-

Table 19-75 Mapping between ICMP names and ICMP types and codes

icmp-name	icmp-type	icmp-code
Echo	8	0
Echo-reply	0	0

 Copyright © Huawei Technologies Co., Ltd.

icmp-name	icmp-type	icmp-code
Parameter-problem	12	0
Port-unreachable	3	3
Protocol-unreachable	3	2
Reassembly-timeout	11	1
Source-quench	4	0
Source-route-failed	3	5
Timestamp-reply	14	0
Timestamp-request	13	0
Ttl-exceeded	11	0
Fragmentneed-DFset	3	4
Host-redirect	5	1
Host-tos-redirect	5	3
Host-unreachable	3	1
Information-reply	16	0
Information-request	15	0
Net-redirect	5	0
Net-tos-redirect	5	2
Net-unreachable	3	0

Views

Advanced ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An advanced ACL matches packets based on information such as source and destination IP addresses, source and destination port numbers, and protocol types.

The **rule** command defines the time range and flexibly configures the time ACL rules take effect.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

An ACL has been created before the rule is configured.

Precautions

- If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.
- To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.
- The ACL with the **vpn-instance** *vpn-instance-name* parameter specified is only applied to firewall and IPSec features.
- To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.
- When you use the **undo rule** command to delete an ACL rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl** command to view the rule ID.
- The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Exercise caution when you run the **undo rule** command.
- When an advanced ACL rule whose ToS value is 1 is configured on the device, fast forwarding is disabled on the interface.
- A port set without port rules cannot be bound to an advanced ACL.
- The protocol type specified in the port set must be the same as the protocol type specified in the advanced ACL.

Example

Add a rule to ACL 3000 to filter ICMP packets.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 1 permit icmp
```

Delete a rule from ACL 3000.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] undo rule 1
```

Add a rule to ACL 3000 to filter IGMP packets.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 2 permit igmp
```

Add a rule to ACL 3000 to filter packets with DSCP priorities.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 3 permit ip dscp cs1
```

Add a rule to ACL 3001 to filter all the IP packets sent from hosts at 10.9.0.0 to hosts at 10.38.160.0.

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule permit ip source 10.9.0.0 0.0.255.255 destination 10.38.160.0 0.0.0.255
```

Add a rule to ACL 3001 to filter the packets with source UDP port number 128 from 10.9.8.0 to 10.38.160.0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule permit udp source 10.9.8.0 0.0.0.255 destination 10.38.160.0 0.0.0.255
destination-port eq 128
```

Add a rule to ACL 3000 to filter tcp-flag packets.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule permit tcp tcp-flag established
```

Related Topics

19.7.4 acl (system view)
19.7.3 acl name
19.7.7 display acl
19.7.23 step

19.7.17 rule (advanced ACL6 view)

Function

The **rule** command adds or modifies an advanced ACL6 rule.

The **undo rule** command deletes an ACL6 rule.

By default, no advanced ACL6 rule is created.

Format

- When **protocol** is set to TCP, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { [**pd** *prefix*] *destination-ipv6-address prefix-length* | [**pd** *prefix*] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **dscp** *dscp* | **precedence** *precedence* | **source** { [**pd** *prefix*] *source-ipv6-address prefix-length* | [**pd** *prefix*] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** | **established** } * | **logging** | **time-range** *time-name* | **tos** *tos*] *
- When **protocol** is set to UDP, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { [**pd** *prefix*] *destination-ipv6-address prefix-length* | [**pd** *prefix*] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **dscp** *dscp* | **precedence** *precedence* | **source** { [**pd** *prefix*] *source-ipv6-address prefix-length* | [**pd** *prefix*] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **logging** | **time-range** *time-name* | **tos** *tos*] *
- When **protocol** is set to ICMPv6, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmpv6** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-*

 Copyright © Huawei Technologies Co., Ltd.

length | **any** } | **dscp** *dscp* | **icmp6-type** { *icmp6-type-name* | *icmp6-type icmp6-code* } | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- When **protocol** is set to IPv6, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **ipv6** } [**destination** { [**pd** *prefix*] *destination-ipv6-address prefix-length* | [**pd** *prefix*] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* } | **dscp** *dscp* | [**fragment** | **none-first-fragment**] | **precedence** *precedence* | **source** { [**pd** *prefix*] *source-ipv6-address prefix-length* | [**pd** *prefix*] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- When GRE or OSPF is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **ospf** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** } | **dscp** *dscp* | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- Rule for deleting an advanced ACL6:

  undo rule *rule-id* [**destination** | **destination-port** | [**fragment** | **none-first-fragment**] | **icmp6-type** | **precedence** | **source** | **source-port** | **logging** | **time-range** | **tos**] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of a rule. • If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. • If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL6 rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step value, the device creates ACL6 rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL6 rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Indicates to drop packets conforming to certain conditions.	-
permit	Indicates to forward packets conforming to certain conditions.	-
tcp	Specifies the protocol type is TCP.	-
udp	Specifies the protocol type is UDP.	-
icmpv6	Specifies the protocol type is ICMPv6.	-
protocol-number	Specifies the protocol type that is expressed as a name or a number.	The value ranges from 1 to 255. The protocol type expressed as a name can be GRE, ICMPv6, IPv6, OSPF, TCP, and UDP.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination { [**pd** *prefix*] *destination-ipv6-address prefix-length* | [**pd** *prefix*] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* }	Indicates the destination address and prefix of a packet. • The **pd** *prefix destination-ipv6-address prefix-length* specifies an IPv6 prefix and a destination IPv6 address, based on which a new IPv6 destination address is calculated through OR operation. An ACL6 rule matches the destination IPv6 addresses of packets against this new IPv6 address. • The **pd** *destination-dhcpv6-prefix* parameter specifies an IPv6 address prefix obtained by a DHCPv6 PD client. An ACL6 rule matches the IPv6 address assigned based on this IPv6 address prefix as the destination IP address of packets.	• The value of *prefix* is a string of 1 to 63 characters. • *destination-ipv6-address* is expressed in hexadecimal notation. The value of *prefix-length* is an integer that ranges from 1 to 128. • **any** represents any source address. • The value of *destination-dhcpv6-prefix* is a string of 1 to 63 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
dscp *dscp*	Specifies the Differentiated Services Code Point (DSCP) value. **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value of *dscp* can be an integer or a name. When the value is an integer, the value ranges from 0 to 63. When the value is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.
logging	Specifies the log recording the IP information, port number, and protocol type of the packets that match the rule. **NOTE** The **logging** only takes effect when the **traffic-filter** command references ACLs.	-
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
none-first-fragment	Indicates that the rule is valid for only non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments. **NOTE** The rules that do not contain **fragment** and **none-first-fragment** parameters are valid for all packets.	-
precedence *precedence*	Indicates that the packets are filtered according to the precedence field.	**precedence** can be expressed as a name or a number. The number ranges from 0 to 7.
source { [**pd** *prefix*] *source-ipv6-address prefix-length* | [**pd** *prefix*] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* }	Indicates the source address and prefix of a packet. • The **pd** *prefix source-ipv6-address prefix-length* specifies an IPv6 prefix and a source IPv6 address, based on which a new IPv6 source address is calculated through OR operation. An ACL6 rule matches the source IPv6 addresses of packets against this new IPv6 address. • The **pd** *source-dhcpv6-prefix* parameter specifies an IPv6 address prefix obtained by a DHCPv6 PD client. An ACL6 rule matches the IPv6 address assigned based on this IPv6 address prefix as the source IP address of packets.	• The value of *prefix* is a string of 1 to 63 characters. • *source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *prefix-length* is an integer that ranges from 1 to 128. • **any** represents any source address. • The value of *source-dhcpv6-prefix* is a string of 1 to 63 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: • **eq** *port*: equivalent to the destination port number. • **gt** *port*: greater than the destination port number. • **1t** *port*: smaller than the destination port number. • **range** *port-start port-end*: destination port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535.
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: • **eq** *port*: equivalent to the source port number. • **gt** *port*: greater than the source port number. • **1t** *port*: smaller than the source port number. • **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
icmp6-type { *icmp6-type-name* | *icmp6-type icmp6-code* }	Indicates that the type and code of ICMPv6 packets, which is effective only when the packet protocol is ICMP. If this parameter is not specified, all ICMP packets are matched.	*icmp6-type*: indicates the type of ICMP messages. The value ranges from 0 to 255. *icmp6-code*: indicates the type of ICMP messages. The value ranges from 0 to 255. The value of *icmp6-type-name* and the corresponding ICMP-Type and ICMP-Code are as **Table 19-76**.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Specifies the type of the SYN Flag in the TCP packet header is ack(010000).	-
fin	Specifies the type of the SYN Flag in the TCP packet header is fin(000001).	-
psh	Specifies the type of the SYN Flag in the TCP packet header is psh(001000).	-
rst	Specifies the type of the SYN Flag in the TCP packet header is rst(000100).	-
syn	Specifies the type of the SYN Flag in the TCP packet header is syn(000010).	-
urg	Specifies the type of the SYN Flag in the TCP packet header is urg(100000).	-
established	Indicates that the SYN Flag type in the TCP packet header is ack(010000) or rst(000100).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-range *time-name*	Indicates that the configured ACL6 rule is effective only in the specified time range. *time-name* indicates the name of the time range during which the ACL6 rule takes effect. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL6, if the specified *time-name* does not exit, the ACL6 does not take effect.	The value of *time-name* is a string of 1 to 32 characters.
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. • The value ranges from 0 to 15 when it is an integer. • When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 19-74** describes the mapping between ToS names and values.

Table 19-76 Values of *icmp6-type-name* and the corresponding ICMP-Type and ICMP-Code

icmp6-type-name	icmp-type	icmp-code
Redirect	137	0
Echo	128	0
Echo-reply	129	0
Err-Header-field	4	0
Frag-time-exceeded	3	1
Hop-limit-exceeded	3	0
Host-admin-prohib	1	1
Host-unreachable	1	3
Neighbor-advertisement	136	0
Neighbor-solicitation	135	0

 Copyright © Huawei Technologies Co., Ltd.

icmp6-type-name	icmp-type	icmp-code
Network-unreachable	1	0
Packet-too-big	2	0
Port-unreachable	1	4
Router-advertisement	134	0
Router-solicitation	133	0
Unknown-ipv6-opt	4	2
Unknown-next-hdr	4	1

Views

Advanced ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Advanced ACL6s classify data packets based on the source IP address, destination IP address, source port number, destination port number, and protocol type.

The **rule** command defines the time range and flexibly configures the time ACL6 rules take effect.

Prerequisites

An ACL6 has been created before the rule is configured.

Precautions

- If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.
- To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.
- To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.
- Only the packet filtering firewall service supports the **rule (advanced ACL6 view)** command to configure ACL6 rules to match the IPv6 address, which is assigned based on the IPv6 address prefix obtained by a DHCPv6 client, as the source or destination IP address of packets. In the same ACL6 rule, **destination pd** *destination-dhcpv6-prefix* and **source pd** *source-dhcpv6-prefix* parameters cannot be configured simultaneously.

 Copyright © Huawei Technologies Co., Ltd.

- When you use the **undo rule** command to delete an ACL6 rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl ipv6** command to view the rule ID.
- The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Exercise caution when you run the **undo rule** command.
- A DHCPv6 PD client does not support the depth first principle.

Example

Add a rule to ACL6 3000 to deny the packets with the source UDP port number that is greater than 128 from fc00:1::1 to fc00:3::1.

```
<Huawei> system-view
[Huawei] acl ipv6 3000
[Huawei-acl6-adv-3000] rule deny udp source fc00:1::1 64 destination fc00:3::1 64 destination-port gt 128
```

Add a rule to ACL6 3000 to filter tcp-flag packets.

```
<Huawei> system-view
[Huawei] acl ipv6 3000
[Huawei-acl6-adv-3000] rule permit tcp tcp-flag established
```

Related Topics

19.7.2 acl ipv6 (system view)

19.7.1 acl ipv6 name

19.7.8 display acl ipv6

19.7.18 rule (basic ACL view)

Function

The **rule** command adds or modifies a basic ACL rule.

The **undo rule** command deletes a basic ACL rule.

By default, no rule is configured for a basic ACL.

Format

rule [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **vpn-instance** *vpn-instance-name* | [**fragment** | **none-first-fragment**] | **logging** | **time-range** *time-name*] *

undo rule *rule-id* [**source** | **logging** | **time-range** | **vpn-instance** | [**fragment** | **none-first-fragment**]] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. • If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. • If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match a rule.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source { *source-address source-wildcard* | **any** }	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. • *source-address*: specifies the source IP address of packets. • *source-wildcard*: specifies the wildcard mask of the source IP address. • **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 or the value of *source-wildcard* is 255.255.255.255.	*source-address* : The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** The ACL with the **vpn-instance** *vpn-instance-name* parameter specified is only applied to the firewall feature.	The value is a string of 1 to 31 characters without spaces. Letters, digits, underscores (_), and dots (.) are allowed.
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-
logging	Specifies the log recording the IP information, port number, and protocol type of the packets that match the rule. **NOTE** The **logging** only takes effect when the **traffic-filter** command references ACLs.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
none-first-fragment	Indicates that the rule is valid for only non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments. **NOTE** The rules that do not contain **fragment** and **none-first-fragment** parameters are valid for all packets.	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.	The value is a string of 1 to 32 characters.

Views

Basic ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A basic ACL matches packets based on information such as source IP addresses, fragment flags, and time ranges.

The **rule** command defines the time range and flexibly configures the time ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.

The ACL with the **vpn-instance** *vpn-instance-name* parameter specified is only applied to the firewall feature.

 Copyright © Huawei Technologies Co., Ltd.

When you use the **undo rule** command to delete an ACL rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl** command to view the rule ID.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Exercise caution when you run the **undo rule** command.

Example

Add a rule in ACL 2001 to permit the packets from 192.168.32.1.

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule permit source 192.168.32.1 0
```

Delete rule 5 from ACL 2001.

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] undo rule 5
```

Related Topics

19.7.4 acl (system view)

19.7.3 acl name

19.7.7 display acl

19.7.23 step

19.7.19 rule (basic ACL6 view)

Function

The **rule** command adds or modifies basic ACL6 rules.

The **undo rule** command deletes an ACL6 rule.

By default, there is no basic ACL6 rule.

Format

rule [*rule-id*] { **deny** | **permit** } [[**fragment** | **none-first-fragment**] | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name*] *

undo rule *rule-id* [[**fragment** | **none-first-fragment**] | **source** | **logging** | **time-range**] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of a rule. • If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. • If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL6 rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step value, the device creates ACL6 rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL6 rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Indicates to drop packets conforming to certain conditions.	-
permit	Indicates to forward packets conforming to certain conditions.	-
logging	Specifies the log recording the IP information, port number, and protocol type of the packets that match the rule. **NOTE** The **logging** only takes effect when the **traffic-filter** command references ACLs.	-
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-
none-first-fragment	Indicates that the rule is valid for only non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments. **NOTE** The rules that do not contain fragment and none-first-fragment parameters are valid for all packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* }	Indicates the source address and prefix of a packet.	*source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *prefix-length* is an integer that ranges from 1 to 128.
any	Indicates any source address.	-
time-range *time-name*	Indicates that the configured ACL6 rule is effective only in the specified time range. *time-name* indicates the name of the time range during which the ACL6 rule takes effect. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL6, if the specified *time-name* does not exit, the ACL6 does not take effect.	The value of *time-name* is a string of 1 to 32 characters.

Views

Basic ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A basic ACL6 matches packets based on information such as source IP addresses, fragment flags, and time ranges.

Prerequisites

An ACL6 has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.

When you use the **undo rule** command to delete an ACL6 rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl ipv6** command to view the rule ID.

 Copyright © Huawei Technologies Co., Ltd.

The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Exercise caution when you run the **undo rule** command.

Example

Add a rule for the ACL6 with a number of 2000 to prohibit the passing of packets from the source fc00:1::1/64.

```
<Huawei> system-view
[Huawei] acl ipv6 2000
[Huawei-acl6-basic-2000] rule deny source fc00:1::1/64
```

Related Topics

19.7.2 acl ipv6 (system view)

19.7.1 acl ipv6 name

19.7.8 display acl ipv6

19.7.20 rule (layer 2 ACL view)

Function

The **rule** command adds or modifies a Layer 2 ACL rule.

The **undo rule** command deletes a Layer 2 ACL rule.

By default, there is no rule in the related Layer 2 ACL view.

Format

rule [*rule-id*] { **permit** | **deny** } [**l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **time-range** *time-name*] *

undo rule *rule-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. • If the specified rule ID has been created, the new rule overwrites the old rule. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. • If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match a rule.	-
permit	Permits the packets that match a rule.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
l2-protocol *type-value* [*type-mask*]	Indicates the type of a Layer 2 protocol. This parameter corresponds to the Ethernet type of Ethernet_II frames and the type-code domain of Ethernet_SNAP frames. • *type-value*: specifies the type value of a Layer 2 protocol. • *type-mask*: specifies the type mask of a Layer 2 protocol.	*type-value* can be a hexadecimal number of 3 to 6 bits that ranges from 0x600 to 0xFFFF or the following protocol name: • ARP, corresponding to 0x0806 • IP, corresponding to 0x0800 • MPLS, corresponding to 0x8847 • RARP, corresponding to 0x8035 The default value of *type-mask* is 0xffff.
destination-mac *dest-mac-address* [*dest-mac-mask*]	Specifies the destination MAC address of packets that matches ACL rules. If the parameter is not specified, packets with any destination address are matched. • *dest-mac-address* specifies the destination MAC address of packets. • *dest-mac-mask* specifies the mask of the destination MAC address of packets.	*dest-mac-address* and *dest-mac-mask* are both in the format of H-H-H. Each H stands for one to four hexadecimal digits. The default value of the *dest-mac-mask* is ffff-ffff-ffff. You can obtain the required destination MAC address range by specifying *source-mac-address* and *source-mac-mask*. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies a MAC address 00e0-fc01-0101, whereas 00e0-fc01-0101 ffff-ffff-0000 specifies a MAC address range from 00e0-fc01-0000 to 00e0-fc01-ffff.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-mac *source-mac-address* [*source-mac-mask*]	Specifies the source MAC address of packets that matches ACL rules. If this parameter is not specified, the packets with any source MAC address are matched. ● *source-mac-address* specifies the source MAC address of packets. ● *source-mac-mask* specifies the mask of the source MAC address of packets. If this parameter is not specified, the mask is ffff-ffff-ffff.	*source-mac-address* and *source-mac-mask* are both in the format of H-H-H. Each H stands for one to four hexadecimal digits. The default value of the *source-mac-mask* is ffff-ffff-ffff. You can obtain the required source MAC address range by specifying *source-mac-address* and *source-mac-mask*. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies a MAC address 00e0-fc01-0101, whereas 00e0-fc01-0101 ffff-ffff-0000 specifies a MAC address range from 00e0-fc01-0000 to 00e0-fc01-ffff.
vlan-id *vlan-id* [*vlan-id-mask*]	Indicates the outer VLAN ID contained in a packet that matches the rule. ● *vlan-id*: specifies the number of the VLAN ID. ● *vlan-id-mask*: specifies the mask of the VLAN ID. If this parameter is not specified, the mask is 0xFFF.	The value of *vlan-id* is an integer ranging from 1 to 4094. The value of the *vlan-id-mask* is a hexadecimal number ranging from 0x0 to 0xFFF. The default value is 0xFFF.
8021p *802.1p-value*	Indicates the 802.1p priority in the outer VLAN tag of a packet that matches the rule.	The value is an integer ranging from 0 to 7.
time-range *time-name*	Defines the time range during which an ACL rule is valid. *time-name* specifies the name of a time range. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.	The value of *time-name* is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

layer 2 ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 ACL matches packets based on Layer 2 information of the packets, such as source MAC addresses, destination MAC addresses, and Layer 2 protocol types.

The **rule** command defines the time range and flexibly configures the time when the ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified rule ID already exists, the new rule overwrites the old rule no matter whether the rules conflict.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.

When you use the **undo rule** command to delete an ACL rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl** command to view the rule ID.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Exercise caution when you run the **undo rule** command.

Example

Add a rule to ACL 4001 to match packets with the destination MAC address being 0000-0000-0001, source MAC address being 0000-0000-0002, and the value of the Layer 2 protocol type being 0x0800.

```
<Huawei> system-view
[Huawei] acl 4001
[Huawei-acl-L2-4001] rule permit destination-mac 0000-0000-0001 source-mac 0000-0000-0002 l2-protocol 0x0800
```

Related Topics

19.7.4 acl (system view)

19.7.3 acl name

19.7.7 display acl

19.7.23 step

 Copyright © Huawei Technologies Co., Ltd.

19.7.21 rule (user ACL view)

Function

The **rule** command configures a user ACL rule.

The **undo rule** command deletes a user ACL rule.

By default, no user ACL rule is configured.

Format

- When the parameter *protocol* is specified as the ICMP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- When the parameter *protocol* is specified as the TCP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- When the parameter *protocol* is specified as the UDP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- When the parameter *protocol* is specified as the GRE, IGMP, IP, IPINIP, or OSPF, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- To delete an ACL rule, run:

  undo rule *rule-id* [**destination** | **destination-port** | **icmp-type** | **source** | **source-port** | **tcp-flag** | **time-range** | **dscp** | **tos** | **precedence** | **fragment**] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. • If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. • If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically start from the step value. The default step is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-
icmp	Indicates that the protocol type is ICMP. The value 1 indicates that ICMP is specified.	-
tcp	Indicates that the protocol type is TCP. The value 6 indicates that TCP is specified.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
udp	Indicates that the protocol type is UDP. The value 17 indicates that UDP is specified.	-
protocol-number	Indicates the protocol type expressed by name or number. **NOTE** Parameters in an ACL vary with the protocol type. The combination of **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } and **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } is applicable to TCP and UDP only.	The value expressed by number is an integer that ranges from 1 to 255. The value expressed by name can be **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **ospf**, **tcp**, or **udp**. **icmp**, **tcp**, **udp**, **gre**, **igmp**, **ipinip**, and **ospf** correspond to 1, 6, 17, 47, 2, 4, and 89.
source { *source-address source-wildcard* | **any** }	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. • *source-address*: specifies the source IP address of packets. • *source-wildcard*: specifies the wildcard mask of the source IP address. • **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 and the value of *source-wildcard* is 255.255.255.255.	*source-address*: The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* }	Indicates the destination IP address of packets that match ACL rules. If this parameter is not specified, packets with any destination IP address are matched. • *destination-address*: specifies the destination IP address of data packets. • *destination-wildcard*: specifies the wildcard mask of the destination IP address. • **any**: indicates any destination IP address of packets. That is, the value of *destination-address* is 0.0.0.0 and the value of *destination-wildcard* is 255.255.255.255. • **passthrough-domain** *domain-string*: indicates the destination domain name of permitted packets. **NOTE** The **passthrough-domain** *domain-string* parameter is valid only when the **permit** parameter is specified.	*destination-address*: The value is in dotted decimal notation. *destination-wildcard*: The value is in dotted decimal notation. The wildcard mask of the destination IP address can be 0, equivalent to 0.0.0.0, indicating that the destination IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1. *domain-string*: The value is a string of 3 to 137 characters. The value of *domain-string* must meet the following requirements: • The value cannot contain two consecutive dots (..). • If you use the fuzzy match function, the first character can be set to *, and * can only be used as the first character of the domain name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
icmp-type { *icmp-name* | *icmp-type icmp-code* }	Indicates the type and code of ICMP packets, which are valid only when the protocol of packets is ICMP. If this parameter is not specified, all types of ICMP packets are matched. • *icmp-name*: specifies the name of ICMP packets. • *icmp-type*: specifies the type of ICMP packets. • *icmp-code*: specifies the code of ICMP packets.	*icmp-type* is an integer that ranges from 0 to 255. *icmp-code* is an integer that ranges from 0 to 255. **NOTE** Table 19-78 lists the mapping between ICMP names and ICMP types and codes.
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: • **eq** *port*: equal operator. • **gt** *port*: greater than operator. • **1t** *port*: smaller than operator. • **range** *port-start port-end*: within the range. *port-start* specifies the start port number, and *port-end* specifies the end port number.	The value of *port* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: • **eq** *port*: equal operator. • **gt** *port*: greater than operator. • **1t** *port*: smaller than operator. • **range** *port-start port-end*: within the range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ack (010000).	-
fin	Indicates that the SYN Flag type in the TCP packet header is fin (000001).	-
psh	Indicates that the SYN Flag type in the TCP packet header is psh (001000).	-
rst	Indicates that the SYN Flag type in the TCP packet header is rst (000100).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
syn	Indicates that the SYN Flag type in the TCP packet header is syn (000010).	-
urg	Indicates that the SYN Flag type in the TCP packet header is urg (100000).	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.	The value is a string of 1 to 32 characters.
dscp *dscp*	Specifies the value of a Differentiated Services Code Point (DSCP). **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value is an integer or a name. • The value ranges from 0 to 63 when it is an integer. • When it is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. • The value ranges from 0 to 15 when it is an integer. • When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 19-77** describes the mapping between ToS names and values.
precedence *precedence*	Indicates that packets are filtered based on the precedence field. *precedence* specifies the precedence value.	The value ranges from 0 to 7. The values 0 to 7 correspond to *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network*.
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-

Table 19-77 Mapping between ToS names and values

ToS Name	Value	ToS Name	Value
normal	0	max-reliability	2
min-monetary-cost	1	max-throughput	4
min-delay	8	-	-

Table 19-78 Mapping between ICMP names and ICMP types and codes

icmp-name	icmp-type	icmp-code
Echo	8	0
Echo-reply	0	0

 Copyright © Huawei Technologies Co., Ltd.

icmp-name	icmp-type	icmp-code
Fragmentneed-DFset	3	4
Host-redirect	5	1
Host-tos-redirect	5	3
Host-unreachable	3	1
Information-reply	16	0
Information-request	15	0
Net-redirect	5	0
Net-tos-redirect	5	2
Net-unreachable	3	0
Parameter-problem	12	0
Port-unreachable	3	3
Protocol-unreachable	3	2
Reassembly-timeout	11	1
Source-quench	4	0
Source-route-failed	3	5
Timestamp-reply	14	0
Timestamp-request	13	0
Ttl-exceeded	11	0

Views

User ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user ACL matches packets based on information such as source IP addresses, destination IP addresses, source port numbers, destination port numbers, and protocol types.

Currently, the user ACL can only be applied to the NAC feature.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

When you use the **undo rule** command to delete an ACL rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl** command to view the rule ID.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Exercise caution when you run the **undo rule** command.

The **passthrough-domain** *domain-string* parameter can specify the name of the domain in which packets can pass. When you attempt to use a UC browser to visit the domain addresses (website addresses) in the whitelist, you may fail to access the websites or response is slow.

Example

Add a rule to ACL 6000 to match all IP packets with destination domain name **www.huawei.com**.

```
<Huawei> system-view
[Huawei] acl 6000
[Huawei-acl-ucl-6000] rule permit ip destination passthrough-domain www.huawei.com
```

Add a rule to ACL 6000 to match all IP packets with destination domain name ***.huawei.com**.

```
<Huawei> system-view
[Huawei] acl 6000
[Huawei-acl-ucl-6000] rule permit ip destination passthrough-domain *.huawei.com
```

Related Topics

19.7.4 acl (system view)

19.7.7 display acl

19.7.22 rule description

Function

The **rule description** command configures the description of an ACL rule.

The **undo rule description** command deletes the description of an ACL rule.

By default, no description is configured for an ACL rule.

Format

rule *rule-id* **description** *description*

undo rule *rule-id* **description**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule.	The value is an integer that ranges from 0 to 4294967294.
description *description*	Specifies the description of an ACL rule. You can configure the description to record an ACL rule in detail.	The value is a character string and contains a maximum of 127 characters.

Views

ACL view, ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

The *rule-id* parameter identifies a rule, but cannot describe the meaning and usage of the rule. The description with a character string can be used to solve the problem.

Prerequisites

The ACL rule has been created. If the ACL rule does not exist, the system displays an error message when you run this command.

Precautions

If the **rule description** command is run repeatedly, the latest configuration takes effect.

After you run the **undo rule** *rule-id* command, the rule and rule description are deleted.

Example

Configure the description for rule 5 in acl 2001, which permits the packets from 192.168.32.1.

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 5 permit source 192.168.32.1 0
[Huawei-acl-basic-2001] rule 5 description permit 192.168.32.1
[Huawei-acl-basic-2001] display acl 2001
Basic ACL 2001, 1 rule
Acl's step is 5
```

 Copyright © Huawei Technologies Co., Ltd.

```
rule 5 permit source 192.168.32.1 0
rule 5 description permit 192.168.32.1
```

Related Topics

19.7.18 rule (basic ACL view)
19.7.16 rule (advanced ACL view)
19.7.20 rule (layer 2 ACL view)
19.7.17 rule (advanced ACL6 view)
19.7.19 rule (basic ACL6 view)
19.7.7 display acl
19.7.8 display acl ipv6

19.7.23 step

Function

The **step** command sets the step between ACL rule IDs.

The **undo step** command restores the default step between ACL rule IDs.

By default, the step between ACL rule IDs is 5.

Format

step *step*

undo step

Parameters

Parameter	Description	Value
step	Specifies the step between ACL rule IDs.	The value is an integer that ranges from 1 to 20.

Views

ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The step is the difference between rule IDs when the system automatically assigns rule IDs. For example, if the ACL step value is set to 5, rules are numbered 5, 10, 15, and so on.

Copyright © Huawei Technologies Co., Ltd.

To add a rule between existing rules, you need to reset the step. For example, an ACL in **config** mode contains three rules with IDs being 5, 10, and 15. To insert a new rule after rule 5 (the first rule), run the **rule 7** *xxxx* command to insert rule 7.

If the step value is changed, ACL rule IDs are arranged automatically. For example, if the original rule IDs are 5, 10, and 15, the rule IDs become 2, 4, and 6 after you change the step value to 2.

NOTE

The **undo step** command can be used to realign ACL rule IDs immediately based on the default step. For example, ACL rule group 3001 contains four rules with IDs being 1, 3, 5, and 7, and the step is 2. After the **undo step** command is executed, the rule IDs become 5, 10, 15, and 20 and the step value is restored to 5.

Prerequisites

An ACL has been created by running the **acl** command.

Example

Set the step between rules in ACL 3101 to 2.

```
<Huawei> system-view
[Huawei] acl 3101
[Huawei-acl-adv-3101] step 2
```

Set the step between rules in ACL6 3101 to 2.

```
<Huawei> system-view
[Huawei] acl ipv6 3101
[Huawei-acl6-adv-3101] step 2
```

Related Topics

19.7.4 acl (system view)

19.7.3 acl name

19.7.24 time-range

Function

The **time-range** command sets a time range.

The **undo time-range** command deletes a time range.

By default, no time range is set.

Format

time-range *time-name* { *start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [**to** *time2 date2*] }

undo time-range *time-name* [*start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [**to** *time2 date2*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
time-name	Specifies the name of a time range.	The value is a string of case-sensitive characters without spaces and must begin with a letter. The value ranges from 1 to 32. To avoid confusion, do not use "all" as the name of a time range.
start-time	Specify the start time of a time range.	The format is hh:mm. • *hh* specifies the hour. The value is an integer that ranges from 0 to 23. • *mm* specifies the minute. The value is an integer that ranges from 0 to 59.
end-time	Specify the end time of a time range.	The format is hh:mm. • *hh* specifies the hour. The value is an integer that ranges from 0 to 23. • *mm* specifies the minute. The value is an integer that ranges from 0 to 59.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
days	Specifies the date on which the time range takes effect.	The value can be one of the following: • The numbers 0 to 6 indicate that the time range takes effect from Sunday to Saturday. The number 0 refers to Sunday. • A weekday includes Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. • The value "Daily" indicates that the time range takes effect during the seven days in a week. • The value "off-day" indicates that the time range takes effect on weekends including Saturday and Sunday. • The value "Working-day" indicates that the time range takes effect in five days from Monday to Friday.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
from *time1 date1*	Specifies the time for the time range to take effect.	*time1* is in the format of hh:mm. • *hh* specifies the hour. The value is an integer that ranges from 0 to 23. • *mm* specifies the minute. The value is an integer that ranges from 0 to 59. *date1* is in the format of yyyy/mm/dd. • *yyyy* specifies the year. The value is an integer that ranges from 1970 to 2099. • *mm* specifies the month. The value is an integer that ranges from 1 to 12. • *dd* specifies the day. The value is an integer that ranges from 1 to 31.
to *time2 date2*	Specifies the end of a time range.	The formats *time2* and *date2* are the same as those of the start time. The end time must be later than the start time. If the end time is not set, the device takes the maximum value allowed by the system.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

If some services or functions need to be started at intervals or periodically, you can run the **time-range** command to set the time range. When configuring ACL or ACL6 rules, you can reference the names of time ranges.

The time range is classified into the following types:

- Relative time range (periodic time range): It is specified by *start-time* and *end-time*. The weekday when the time range takes effect is determined by *days*.
- Absolute time range: It is specified by **from** and **to**. The absolute time range can be used to limit the periodic time range.

You can set the same name for multiple time ranges to describe a special period. If multiple time ranges have the same name, the periodic time ranges are ORed, and a periodic time range and a definite time range are ANDed. For example, three time ranges are set with the same name **test**:

- Time range 1: 01.01.2010 00:00 to 31.12.2010 23:59 (absolute time range)
- Time range 2: 8:00 to 18:00 from Monday to Friday (periodic time range)
- Time range 3: 14:00 to 18:00 on Saturday and Sunday (periodic time range)

The time range **test** takes effect at 8:00-18:00 on Monday to Friday and 14:00-18:00 on Saturday and Sunday in the year 2010.

Precautions

Deleting the time range in use may affect the ACL rule referenced by the time range. Therefore, use this command with caution.

If a router (AR100, AR120, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L) restarts unexpectedly, the system time is restored to factory setting. After the router restarts, set the system time correctly; otherwise, the command cannot be run.

Example

Set a time range named **test** that takes effect from 2010-01-01 00:00 to 2010-12-31 23:59.

```
<Huawei> system-view
[Huawei] time-range test from 0:0 2010/1/1 to 23:59 2010/12/31
```

Set a time range named **test** that takes effect at 8:00-18:00 from Monday to Friday.

```
<Huawei> system-view
[Huawei] time-range test 8:00 to 18:00 working-day
```

Set a time range named **test** that takes effect from 14:00 to 18:00 on every Saturday and Sunday.

```
<Huawei> system-view
[Huawei] time-range test 14:00 to 18:00 off-day
```

Related Topics

19.7.10 display time-range

 Copyright © Huawei Technologies Co., Ltd.

19.8 Firewall Configuration Commands

19.8.1 bypass

Function

The **bypass** command enables the packet filtering firewall bypass function in an interzone.

The **undo bypass** command disables the packet filtering firewall bypass function in an interzone.

By default, the packet filtering firewall bypass function is disabled in an interzone.

Format

bypass [**session-overrun**]

undo bypass

Parameters

Parameter	Description	Value
session-overrun	Configures the device to create a flow table and forward traffic based on the flow table before the number of flow tables reaches the upper limit, and to create no flow table and forward traffic based on the interzone ACL policy after the number of flow tables reaches the upper limit. If this parameter is not specified, the device does not create a flow table and forwards traffic based on the interzone ACL policy.	-

Views

Interzone view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

A packet filtering firewall builds a flow table based on source IP addresses, source ports, destination IP addresses, destination ports, and transport-layer protocol. There is a limit on the flow table size since it occupies memory resources. If the flow table size reaches the limit, traffic of new services will fail to be forwarded because they cannot obtain flow table resources. To address this issue, configure the packet filtering firewall bypass function in an interzone. This configuration allows traffic to be forwarded based on inter-zone ACL rules, without the need of building flow table entries.

NOTE

After the packet filtering firewall bypass function is configured, the firewall supports only the packet filtering and packet filtering log functions.

Example

Enable the packet filtering firewall bypass function in the interzone between zone1 and zone2.

```
<Huawei> system-view
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] bypass
```

19.8.2 clear firewall statistics system

Function

The **clear firewall statistics system** command clears the statistics about normal packets in the system.

Format

clear firewall statistics system normal

Parameters

Parameter	Description	Value
normal	Indicates the statistics about normal packets.	-

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To view the communication packets of a device within a specified period, run the **clear firewall statistics system normal** command to clear the previous packet statistics on the device first.

Example

Clear the statistics about normal packets in the system.

```
<Huawei> system-view
[Huawei] clear firewall statistics system normal
```

19.8.3 clear firewall statistics zone

Function

The **clear firewall statistics zone** command clears the statistics about normal packets in a zone.

Format

clear firewall statistics zone *zone-name*

Parameters

Parameter	Description	Value
zone-name	Specifies the name of a zone.	The value must be the name of an existing zone.

Views

System view

Default Level

3: Management level

Usage Guidelines

To view the packets in a zone within a specified period, run the **clear firewall statistics zone** command to clear the previous packet statistics in the zone first.

Example

Clear the statistics about normal packets in the zone **zone1**.

```
<Huawei> system-view
[Huawei] clear firewall statistics zone zone1
```

 Copyright © Huawei Technologies Co., Ltd.

19.8.4 detect aspf

Function

The **detect aspf** command enables application specific packet filter (ASPF) in an interzone.

The **undo detect aspf** command disables ASPF in an interzone.

By default, ASPF is disabled in an interzone.

Format

detect aspf { **ftp** | **rtsp** | **sip** }

undo detect aspf { **ftp** | **rtsp** | **sip** }

Parameters

Parameter	Description	Value
ftp	Applies ASPF to the FTP protocol packets.	-
rtsp	Applies ASPF to the RTSP protocol packets.	-
sip	Applies ASPF to the SIP protocol packets.	-

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ASPF filters application-layer protocol packets. It is a status-based packet filtering method. ASPF can detect the sessions that attempt to traverse the application layer and deny the undesired packets.

Prerequisites

An interzone has been created using the **firewall interzone** command.

Example

Enable ASPF in the interzone between **zone1** and **zone2**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone2-zone1] detect aspf ftp
```

Related Topics

19.8.10 display firewall interzone

19.8.5 display firewall app session table

Function

The **display firewall app session table** command displays the application session table.

Format

display firewall app session table [**application-protocol** { **dns** | **ftp** | **http** | **pptp** | **rtsp** | **sip** }] [**source-ip** *ip-address* [*port-number*]] [**destination-ip** *ip-address* [*port-number*]]

Parameters

Parameter	Description	Value
application-protocol	Indicates the type of the application-layer protocol.	-
dns	Displays the application session table information of DNS packets.	-
ftp	Displays the application session table information of FTP packets.	-
http	Displays the application session table information of HTTP packets.	-
pptp	Displays the application session table information of PPTP packets.	-
rtsp	Displays the application session table information of RTSP packets.	-
sip	Displays the application session table information of SIP packets.	-
source-ip *ip-address*	Indicates the source IP address of flows.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination-ip *ip-address*	Indicates the destination IP address of flows.	The value is in dotted decimal notation.
port-number	Indicates the port number.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display firewall app session table** command displays information about a specified application session table or all application session tables. The application session table information is displayed only when some traffic is sent to the application layer.

Example

Display information about all application session tables.

```
<Huawei> display firewall app session table
 The total number of session tables is 1.
  NO.1.
    APP-Protocol : RTSP
    Initiator-VPN: ----
    Responder-VPN: ----
    Connection Info:
      Initiator(IP:Port)         Responder(IP:Port)     Protocol
      10.7.11.2       :33713 ---> 10.5.11.2       :554   TCP(6)
      10.7.11.2       :33713 <--- 10.5.11.2       :554   TCP(6)
```

Table 19-79 Description of the display firewall app session table command output

Item	Description
NO.1.	The first entry in the session table.
APP-Protocol : RTSP	The application protocol is RTSP.
Initiator-VPN: ----	Source VPN name.
Responder-VPN: ----	Destination VPN name.
Connection Info:	Connection between source address and destination address.
Initiator(IP:Port)	Source IP address and port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Responder(IP:Port)	Destination IP address and port number.
Protocol	Transport protocol type (TCP/UDP).

19.8.6 display firewall app table statistics

Function

The **display firewall app table statistics** command displays statistics on firewall application entries.

Format

display firewall app { **servermap** | **session** } **table statistics**

Parameters

Parameter	Description	Value
servermap	Displays statistics on servermap entries at the application layer.	-
session	Displays statistics on session entries at the application layer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view statistics on firewall Session entries and Servermap entries to facilitate firewall related fault diagnosis and troubleshooting.

Session entry: includes quintuple information (the protocol number, source IP address, source port number, destination IP address, and destination port number). When each session passes through the firewall, a session entry is created on the firewall.

Servermap entry: includes triplet information (the protocol number, source IP address, and destination IP address). When the firewall uses a multi-channel protocol for communication, Servermap entries are created.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display statistics on all session entries at the application layer.

```
<Huawei> display firewall app session table statistics
 App-inspect Session History Maximum Info:
 Maximum Number :115
 Record Time    :2013-09-22 12:19:05
```

Table 19-80 Description of the display firewall app session table statistics command output

Item	Description
App-inspect Session History Maximum Info	Information about maximum number of session entries in the history.
Maximum Number	Maximum number of session entries.
Record Time	Time when maximum number of session entries is recorded.

Display statistics on all Servermap entries at the application layer.

```
<Huawei> display firewall app servermap table statistics
 App-inspect Servermap History Maximum Info:
 Maximum Number :115
 Record Time    :2013-09-22 12:19:31
```

Table 19-81 Description of the display firewall app servermap table statistics command output

Item	Description
App-inspect Servermap History Maximum Info	Information about maximum number of Servermap entries in the history.
Maximum Number	Maximum number of Servermap entries.
Record Time	Time when maximum number of Servermap entries is recorded.

Related Topics

19.8.66 reset firewall app table statistics

19.8.7 display firewall blacklist

Function

The **display firewall blacklist** command displays the blacklist entries.

 Copyright © Huawei Technologies Co., Ltd.

Format

display firewall blacklist { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **dynamic** | **static** | **vpn-instance** *vpn-instance-name* }

Parameters

Parameter	Description	Value
all	Displays all the blacklist entries.	-
ip-address	Displays the blacklist entry matching a specified IP address.	The value is a valid IPv4 IP address.
dynamic	Displays the dynamic blacklist entries.	-
static	Displays the static blacklist entries.	-
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all the blacklist entries.

```
<Huawei> display firewall blacklist all
Firewall blacklist items :
------------------------------------------------------------------------------
IP-Address      Reason       Expire-Time(m)    VPN-Instance
------------------------------------------------------------------------------
10.1.1.1        Manual       100
------------------------------------------------------------------------------
 Total number is : 1
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-82 Description of the display firewall blacklist command output

Item	Description
IP-Address	IP address in a blacklist entry.
Reason	Reason why a blacklist entry is generated, including: • IPSweep: The entry is generated because of an IP address sweeping attack. • Manual: The entry is added to the blacklist manually. • PortScan: The entry is generated because of a port scanning attack.
Expire-Time(m)	Aging time of a blacklist entry. m indicates minute. If the *Permanent* keyword is used, the entry will be valid permanently. To configure a blacklist entry, run the **firewall blacklist** command.
VPN-Instance	Name of the VPN instance that the IP address in a blacklist entry belongs to.
Total number is : 1	There is a total of one entry in the blacklist.

Related Topics

19.8.22 firewall blacklist

19.8.8 display firewall blacklist configuration

Function

The **display firewall blacklist configuration** command displays the status of the blacklist function.

Format

display firewall blacklist configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Check whether the blacklist function is enabled on the device.

```
<Huawei> display firewall blacklist configuration
Info:Blacklist is disabled.
```

Table 19-83 Description of the display firewall blacklist configuration command output

Item	Description
Info:Blacklist is disabled	The blacklist function is disabled. To enable the blacklist function, run the **firewall blacklist enable** command.

Related Topics

19.8.23 firewall blacklist enable

19.8.9 display firewall defend

Function

The **display firewall defend** command displays the status and configurations of the attack defense functions. For the Flood attack defense function, you can also view the attack defense configuration of the specified zone or IP address.

Format

display firewall defend { **flag** | { **icmp-flood** | **syn-flood** | **udp-flood** } [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]] | *other-attack-type* }

Parameters

Parameter	Description	Value
flag	Displays the status of all the attack defense functions.	-
icmp-flood	Displays the configuration of the ICMP Flood attack defense.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
syn-flood	Displays the configuration of the SYN Flood attack defense.	-
udp-flood	Displays the configuration of the UDP Flood attack defense.	-
ip [*ip-address*]	Displays the Flood attack defense function configured for the specified IP address.	The value is a valid IPv4 IP address.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.
zone [*zone-name*]	Displays the Flood attack defense function configured for the specified zone.	The value of *zone-name* is a string of 1 to 32 case-sensitive characters. It must be an existing zone name.
other-attack-type	Displays the configurations of other attack defense except for the Flood attack defense.	The other types of attacks include: • fraggle • icmp-redirect • icmp-unreachable • ip-fragment • ip-sweep • land • large-icmp • ping-of-death • port-scan • smurf • tcp-flag • teardrop • tracert • winnuke

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the status of each attack defense function.

```
<Huawei> display firewall defend flag
---------------------------------
  Type                  Flag
---------------------------------
  land                : disable
  smurf               : disable
  fraggle             : disable
  winnuke             : disable
  syn-flood           : disable
  udp-flood           : disable
  icmp-flood          : disable
  icmp-redirect       : disable
  icmp-unreachable    : disable
  ip-sweep            : disable
  port-scan           : disable
  tracert             : disable
  ping-of-death       : disable
  teardrop            : disable
  tcp-flag            : disable
  ip-fragment         : disable
  large-icmp          : disable
---------------------------------
```

Display the configuration of IP address sweeping attack defense.

```
<Huawei> display firewall defend ip-sweep

  defend-flag          : disable
  max-rate             : 4000  (pps)
  blacklist-expire-time : 20    (m)
```

Table 19-84 Description of the display firewall defend command output

Item	Description
Type	Type of attacks to defend against.
Flag	Flag indicating whether attack defense is enabled. • disable: Attack defense is disabled. • enable: Attack defense is enabled.
defend-flag	Flag indicating whether attack defense is enabled. • disable: Attack defense is disabled. • enable: Attack defense is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
max-rate	Maximum session rate of address scanning attack defense, in pps. To set the maximum session rate of address scanning attack defense, run the **firewall defend ip-sweep** command.
blacklist-expire-time	Timeout interval of the blacklist. To set the timeout interval of the blacklist, run the **firewall defend ip-sweep** command.

19.8.10 display firewall interzone

Function

The **display firewall interzone** command displays information about an interzone.

Format

display firewall interzone [*zone-name1 zone-name2*]

Parameters

Parameter	Description	Value
zone-name1	Specifies the name of a zone included in the interzone.	The name is a string of 1 to 32 case-sensitive characters. *zone-name1* must be a zone name created by the **19.8.59 firewall zone** command.
zone-name2	Specifies the name of a zone included in the interzone.	The name is a string of 1 to 32 case-sensitive characters. *zone-name2* must be a zone name created by the **19.8.59 firewall zone** command.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can use the **display firewall interzone** command to obtain information about an interzone.

Example

Display information about the interzone between **zone1** and **zone2**.

```
<Huawei> display firewall interzone zone1 zone2
interzone zone2 zone1
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 session-log 3000 inbound
 detect aspf ftp
 bypass
<Huawei> display firewall interzone zone1 zone2
interzone zone2 zone1
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3000 inbound
 packet-filter logging inbound permit
 bypass session-overrun
```

Table 19-85 Description of the display firewall interzone command output

Item	Description
interzone zone2 zone1	Interzone between two zones. To configure an interzone, run the **firewall interzone** command.
firewall enable	Firewall function is enabled in the interzone. To enable the firewall function, run the **firewall enable** command.
session-log 2006 inbound	Firewall logs are recorded based on filtering rules in ACL 2006. To reference an ACL, run the **session-log** command.
packet-filter default permit inbound	Default inbound packet filtering rule in an interzone: permit. To configure a packet filtering rule, run the **packet-filter** command.
packet-filter default deny outbound	Default outbound packet filtering rule in an interzone: deny. To configure a packet filtering rule, run the **packet-filter** command.
detect aspf ftp	ASPF is enabled for FTP packets. To enable ASPF, run the **detect aspf** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
packet-filter logging inbound permit	Packet filtering log function. To configure the packet filtering log function, run the **packet-filter logging** command.
bypass/bypass session-overrun	The packet filtering firewall bypass function is enabled in an interzone. To enable this function, run the **bypass** command.

Related Topics

19.8.51 firewall interzone
19.8.50 firewall enable
19.8.61 packet-filter
19.8.4 detect aspf

19.8.11 display firewall ipv6 session

Function

The **display firewall ipv6 session** command displays the IPv6 session table of the firewall.

Format

display firewall ipv6 session { **all** [**verbose**] | **number** }

display firewall ipv6 session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display firewall ipv6 session destination *destination-address* [*destination-port*] [**verbose**]

display firewall ipv6 session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all session table information.	-
verbose	Displays detailed information about the session table.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
number	Displays the number of entries in the session table.	-
protocol { *protocol-number* | *protocol-name* }	Displays the entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMPv6, TCP, or UDP.
source *source-address* [*source-port*]	Displays the entries with a specified source IPv6 address or both a source IPv6 address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• The total length of *source-address* is 128 bits. The string is divided into 8 groups, each of which consists of 4 hexadecimal digits. The value is in format X:X:X:X:X:X:X:X. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address*[*destination-port*]	Displays the entry with a specified destination IPv6 address or both a destination IPv6 address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• The total length of *destination-address* is 128 bits. The string is divided into 8 groups, each of which consists of 4 hexadecimal digits. The value is in format X:X:X:X:X:X:X:X. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run this command to check information about a firewall session table.

Example

Display the number of IPv6 entries in the session table.

```
<Huawei> display firewall ipv6 session number
 The total number of firewall ipv6 session tables is: 1
```

Display details about all IPv6 entries in the session table.

```
<Huawei> display firewall ipv6 session all verbose
  Firewall Ipv6 Session Table Information:
     Protocol          : TCP(6)
     SrcAddr  Port Vpn : fe80::1          1
     DestAddr Port Vpn : fc00::1          1
     Time To Live      : 120 s
     Firewall-Info
       InZone          : untrust
       OutZone         : trust
  Total : 1
```

Table 19-86 Description of the **display firewall session all verbose** command output

Item	Description
Firewall Ipv6 Session Table Information	IPv6 session table information.
Protocol	Protocol type.
SrcAddr Port Vpn	Source address, service port number, and VPN instance name.
DestAddr Port Vpn	Destination address, service port number, and VPN instance name.
Time To Live	Lifetime of the session table entries.
Firewall-Info	Firewall information.
InZone	Inzone name.
OutZone	Outzone name.
Total	Number of entries in the session table.

19.8.12 display firewall log configuration

Function

The **display firewall log configuration** command displays the global configuration of the firewall logging functions.

 Copyright © Huawei Technologies Co., Ltd.

Format

display firewall log configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the global configuration of the firewall logging functions.

```
<Huawei> display firewall log configuration
defend log :
  status : enabled
  log-interval : 30 s
statistics log :
  status : enabled
  log-interval : 30 s
blacklist log :
  status : enabled
  log-interval : 30 s
session log :
  status : enabled
  log-interval : 30 s
  nat-session : disabled
binary-log host :
  host                 source               VPN instance-name
  ----:--              ----:--              ---
packet filter log :
  status : disabled
  log-interval : 30 s
```

Table 19-87 Description of the display firewall log configuration command output

Item	Description
status	Status of a firewall logging function. **enable** indicates that the logging function is enabled; **disable** indicates that the logging function is disabled.
log-interval	Interval for exporting logs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
nat-session	Status of NAT session logs. **enable** indicates that the logging function is enabled; **disable** indicates that the logging function is disabled.
host	IP address and port number of the log server.
source	IP address and port number used by the device to communicate with the log server.
VPN instance-name	Name of a VPN instance.

Related Topics

19.8.53 firewall log enable
19.8.54 firewall log log-interval
19.8.52 firewall log binary-log host
19.8.55 firewall log session nat enable

19.8.13 display firewall session

Function

The **display firewall session** command displays the firewall session table.

Format

display firewall session { **all** [**verbose**] | **number** }

display firewall session destination *destination-address* [*destination-port*] [**verbose**]

display firewall session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display firewall session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all entries in the firewall session table.	-
verbose	Displays details about the firewall session table.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
number	Displays the number of entries in the firewall session table.	-
protocol { *protocol-number* | *protocol-name* }	Displays entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMP, TCP, or UDP.
source *source-address* [*source-port*]	Displays entries with a specified source IP address or both a source IP address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• *source-address* is in dotted decimal notation. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address*[*destination-port*]	Displays entries with a specified destination IP address or both a destination IP address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• *destination-address* is in dotted decimal notation. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run this command to check information about a firewall session table.

Example

Display the number of entries in the session table.

```
<Huawei> display firewall session number
 The total number of firewall session tables is: 1
```

Display details about all entries in the session table.

```
<Huawei> display firewall session all verbose
  Firewall Session Table Information:
    Protocol          : TCP(6)
    SrcAddr  Port Vpn : 10.6.34.204    114   vpn1
    DestAddr Port Vpn : 10.1.1.1        21
    Time To Live      : 120 s
    Firewall-Info
      InZone          : a
      OutZone         : b

 Total : 1
```

Table 19-88 Description of the display firewall session all verbose command output

Item	Description
Protocol	Protocol type.
SrcAddr Port Vpn	Source address, service port number, and VPN instance name.
DestAddr Port Vpn	Destination address, service port number, and VPN instance name.
Time To Live	Lifetime of the session table entries.
Firewall-Info	Firewall information.
InZone	Inbound zone name.
OutZone	Outbound zone name.
Total	Number of entries in the firewall session table.

19.8.14 display firewall statistics system

Function

The **display firewall statistics system** command displays traffic statistics on the firewall.

Format

display firewall statistics system [**normal all** | **defend**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
normal all	Displays the statistics about packets passing the firewall.	-
defend	Displays the statistics about attack packets passing the firewall.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **display firewall statistics system** command without specifying any parameters, the upper and lower thresholds for controlling the TCP, UDP, ICMP, TCP proxy, and IP fragment packets (session number) are displayed.

Example

Display the global traffic thresholds set on the firewall.

```
<Huawei> display firewall statistics system
------------------------------------------------------------------------
            Global system statistics config information
------------------------------------------------------------------------
 Is enable          0                <enable : 1  disable : 0 >
----------------------------------High----------------------Low-------
Tcp connect-number              16384                  12288

Udp connect-number              16384                  12288

Icmp connect-number             16384                  12288

Tcp-proxy connect-number        16384                  12288

Frag connect-number             16384                  12288

------------------------------------------------------------------------
```

Display the statistics of packets passing the firewall.

```
<Huawei> display firewall statistics system normal all
IPv4 statistics:
HistoryTcpTotal-------------0
CurTcpTearTotal-------------0
HistoryUdpTotal-------------0
CurUdpTearTotal-------------0
HistoryIcmpTotal------------0
CurIcmpTearTotal------------0
HisTcpProxyTotal------------0
CurTcpProxyTearTotal--------0
```

 Copyright © Huawei Technologies Co., Ltd.

```
HistoryFragTotal------------0
CurFragTearTotal------------0
IPv6 statistics:
HistoryIPv6Total------------0
CurTcpIPv6TearTotal---------0
HistoryUdpIPv6Total---------0
CurUdpIPv6TearTotal---------0
HistoryIcmpV6Total----------0
CurIcmpV6TearTotal----------0
HistoryIPv6FragTotal--------0
CurIPv6FragTearTotal--------0
```

Table 19-89 Description of the display firewall statistics system normal all command output

Item	Description
IPv4 statistics:	IPv4 traffic statistics on the firewall.
HistoryTcpTotal	Number of historical TCP connections.
CurTcpTearTotal	Number of TCP current connections.
HistoryUdpTotal	Number of history UDP connections.
CurUdpTearTotal	Number of UDP current connections.
HistoryIcmpTotal	Number of history ICMP connections.
CurIcmpTearTotal	Number of ICMP current connections.
HisTcpProxyTotal	Number of historical TCP proxy connections.
CurTcpProxyTearTotal	Number of TCP current proxy connections.
HistoryFragTotal	Number of historical fragment flow entries.
CurFragTearTotal	Number of current fragment flow entries.
IPv6 statistics:	IPv6 traffic statistics on the firewall.
HistoryIPv6Total	Number of historical TCP IPv6 connections.
CurTcpIPv6TearTotal	Number of TCP IPv6 connections that are torn down.
HistoryUdpIPv6Total	Number of historical UDP IPv6 connections.
CurUdpIPv6TearTotal	Number of UDP IPv6 connections that are torn down.
HistoryIcmpV6Total	Number of historical ICMPv6 connections
CurIcmpV6TearTotal	Number of ICMPv6 connections that are torn down.
HistoryIPv6FragTotal	Number of historical IPv6 fragment flow entries.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CurIPv6FragTearTotal	Number of current IPv6 fragment flow entries.

Display the statistics on attack packets passing the firewall.

```
<Huawei> display firewall statistics system defend
 --------------------FW GLOBAL DEFEND TABLE---------------------
DropID[710]             0 FW_INTERZONE_DENY_DROP
DropID[715]             0 FW_ACL_FILTER_DENY_DROP
DropID[736]             0 FW_GLOBAL_UDP_CONNECT_DROP
DropID[737]             0 FW_GLOBAL_TCP_CONNECT_DROP
DropID[738]             0 FW_GLOBAL_ICMP_CONNECT_DROP
DropID[739]             0 FW_GLOBAL_TCP_PROXY_CONNECT_DROP
DropID[740]             0 FW_ZONE_IN_UDP_CONNECT_DROP
DropID[741]             0 FW_ZONE_OUT_UDP_CONNECT_DROP
DropID[742]             0 FW_ZONE_IN_TCP_CONNECT_DROP
DropID[743]             0 FW_ZONE_OUT_TCP_CONNECT_DROP
DropID[744]             0 FW_ZONE_IN_ICMP_CONNECT_DROP
DropID[745]             0 FW_ZONE_OUT_ICMP_CONNECT_DROP
DropID[746]             0 FW_ZONE_IP_IN_UDP_CONNECT_DROP
DropID[747]             0 FW_ZONE_IP_OUT_UDP_CONNECT_DROP
DropID[748]             0 FW_ZONE_IP_IN_TCP_CONNECT_DROP
DropID[749]             0 FW_ZONE_IP_OUT_TCP_CONNECT_DROP
DropID[750]             0 FW_ZONE_IP_IN_ICMP_CONNECT_DROP
DropID[751]             0 FW_ZONE_IP_OUT_ICMP_CONNECT_DROP
DropID[752]             0 FW_GLOBAL_FRAG_CONNECT_DROP
DropID[764]             0 FW_LAND_DEFEND_DROP
DropID[765]             0 FW_SMURF_DEFEND_DROP
DropID[766]             0 FW_FRAGGLE_DEFEND_DROP
DropID[767]             0 FW_WINNUKE_DEFEND_DROP
DropID[768]             0 FW_CONNECT_SYNFLOOD_DEFEND_DROP
DropID[769]             0 FW_CONNECT_ICMPFLOOD_DEFEND_DROP
DropID[770]             0 FW_CONNECT_UDPFLOOD_DEFEND_DROP
DropID[771]             0 FW_ICMPREDIRECT_DEFEND_DROP
DropID[772]             0 FW_ICMPUNREACHABLE_DEFEND_DROP
DropID[773]             0 FW_IPSWEEP_DEFEND_DROP
DropID[774]             0 FW_PORTSCAN_DEFEND_DROP
DropID[775]             0 FW_TRACERT_DEFEND_DROP
DropID[776]             0 FW_PINGOFDEATH_DEFEND_DROP
DropID[777]             0 FW_TEARDROP_DEFEND_DROP
DropID[778]             0 FW_TCPFLAG_DEFEND_DROP
DropID[779]             0 FW_IPFRAGMENT_DEFEND_DROP
DropID[780]             0 FW_LARGEICMP_DEFEND_DROP
DropID[781]             0 FW_BLACKIPLIST_DEFEND_DROP
DropID[782]             0 FW_FLOW_SYNFLOOD_DEFEND_DROP
DropID[783]             0 FW_FLOW_ICMPFLOOD_DEFEND_DROP
DropID[784]             0 FW_FLOW_UDPFLOOD_DEFEND_DROP
DropID[785]             0 FW_FRAG_SESSION_NUM_OVER_DROP
DropID[786]             0 FW_TEARDROP_BAD_IPLEN_DROP
```

Table 19-90 Description of the display firewall statistics system defend command output

Item	Description
FW_INTERZONE_DENY_DROP	Number of packets rejected by the firewall.
FW_ACL_FILTER_DENY_DROP	Number of packets rejected by the ACL.
FW_GLOBAL_UDP_CONNECT_DROP	Number of discarded packets of excess global UDP connections.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
FW_GLOBAL_TCP_CONNECT_DROP	Number of discarded packets of excess global TCP connections.
FW_GLOBAL_ICMP_CONNECT_DROP	Number of discarded packets of excess global ICMP connections.
FW_GLOBAL_TCP_PROXY_CONNECT_DROP	Number of discarded packets of excess global split TCP proxy connections initiated globally.
FW_ZONE_IN_UDP_CONNECT_DROP	Number of discarded incoming packets of excess UDP connections in a zone.
FW_ZONE_OUT_UDP_CONNECT_DROP	Number of discarded outgoing packets of excess UDP connections.
FW_ZONE_IN_TCP_CONNECT_DROP	Number of discarded incoming packets of excess TCP connections in a zone.
FW_ZONE_OUT_TCP_CONNECT_DROP	Number of discarded outgoing packets of excess TCP connections in a zone.
FW_ZONE_IN_ICMP_CONNECT_DROP	Number of discarded incoming packets of excess ICMP connections.
FW_ZONE_OUT_ICMP_CONNECT_DROP	Number of discarded outgoing packets of excess ICMP connections in a zone.
FW_ZONE_IP_IN_UDP_CONNECT_DROP	Number of discarded incoming packets of excess UDP connections.
FW_ZONE_IP_OUT_UDP_CONNECT_DROP	Number of discarded outgoing packets of excess UDP connections.
FW_ZONE_IP_IN_TCP_CONNECT_DROP	Number of discarded incoming packets of excess TCP connections.
FW_ZONE_IP_OUT_TCP_CONNECT_DROP	Number of discarded outgoing packets of excess TCP connections.
FW_ZONE_IP_IN_ICMP_CONNECT_DROP	Number of discarded incoming packets of excess ICMP connections.
FW_ZONE_IP_OUT_ICMP_CONNECT_DROP	Number of discarded outgoing packets of excess ICMP connections.
FW_GLOBAL_FRAG_CONNECT_DROP	Number of discarded packets of excess fragment connections initiated globally.
FW_LAND_DEFEND_DROP	Number of discarded Land attack packets.
FW_SMURF_DEFEND_DROP	Number of discarded Smurf attack packets.
FW_FRAGGLE_DEFEND_DROP	Number of discarded Fraggle attack packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
FW_WINNUKE_DEFEND_DROP	Number of discarded Winnuke attack packets.
FW_CONNECT_SYNFLOOD_DEFEND_DROP	Number of discarded initial packets of SYN flood attacks.
FW_CONNECT_ICMPFLOOD_DEFEND_DROP	Number of discarded initial packets of ICMP flood attacks.
FW_CONNECT_UDPFLOOD_DEFEND_DROP	Number of discarded initial packets of UDP flood attacks.
FW_ICMPREDIRECT_DEFEND_DROP	Number of discarded ICMP redirection attack packets.
FW_ICMPUNREACHABLE_DEFEND_DROP	Number of discarded ICMP unreachable attack packets.
FW_IPSWEEP_DEFEND_DROP	Number of discarded IP scanning attack packets.
FW_PORTSCAN_DEFEND_DROP	Number of discarded port scanning attack packets.
FW_TRACERT_DEFEND_DROP	Number of discarded Tracert attack packets.
FW_PINGOFDEATH_DEFEND_DROP	Number of discarded ping of death attack packets.
FW_TEARDROP_DEFEND_DROP	Number of discarded Teardrop attack packets.
FW_TCPFLAG_DEFEND_DROP	Number of discarded malformed TCP attack packets.
FW_IPFRAGMENT_DEFEND_DROP	Number of discarded IP fragment attack packets.
FW_LARGEICMP_DEFEND_DROP	Number of discarded large-sized ICMP attack packets.
FW_BLACKIPLIST_DEFEND_DROP	Number of discarded blacklisted attack packets.
FW_FLOW_SYNFLOOD_DEFEND_DROP	Number of discarded non-initial SYN flood attack packets.
FW_FLOW_ICMPFLOOD_DEFEND_DROP	Number of discarded non-initial ICMP flood attack packets.
FW_FLOW_UDPFLOOD_DEFEND_DROP	Number of discarded non-initial UDP flood attack packets.
FW_FRAG_SESSION_NUM_OVER_DROP	Number of discarded excess fragments.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
FW_TEARDROP_BAD_IPLEN_DROP	Number of discarded invalid packets.

Related Topics

19.8.56 firewall statistics system connect-number

19.8.15 display firewall statistics zone

Function

The **display firewall statistics zone** command displays traffic statistics and monitoring information in a zone.

Format

display firewall statistics zone *zone-name* { **inzone** | **outzone** } **all**

Parameters

Parameter	Description	Value
zone-name	Indicates the name of a zone.	The value must be the name of an existing zone.
inzone	Displays the statistics about the traffic entering the zone.	-
outzone	Displays the statistics about the traffic leaving the zone.	-
all	Displays the statistics about the traffic entering and leaving the zone.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **display firewall statistics zone** command displays the number of current sessions and historical sessions in the inbound or outbound direction of a zone and the number of HTTP, FTP, or DNS packets in a certain direction.

Example

Display the inbound packet statistics of zone1.

```
<Huawei> display firewall statistics zone zone1 inzone all
ZoneID:0  Direction:IN
InTcpSetupTotal-----------------0
InTcpTearTotal------------------0
InUdpSetupTotal-----------------0
InUdpTearTotal------------------0
InIcmpSetupTotal----------------0
InIcmpTearTotal-----------------0
```

Display the outbound packet statistics of zone1.

```
<Huawei> display firewall statistics zone zone1 outzone all
ZoneID:0  Direction:OUT
OutTcpSetupTotal----------------0
OutTcpTearTotal-----------------0
OutUdpSetupTotal----------------0
OutUdpTearTotal-----------------0
OutIcmpSetupTotal---------------0
OutIcmpTearTotal----------------0
```

Table 19-91 Description of the display firewall statistics zone command output

Item	Description
InTcpSetupTotal / OutTcpSetupTotal	Number of TCP connections in inbound and outbound directions.
InTcpTearTotal / OutTcpTearTotal	Number of deleted TCP connections in inbound and outbound directions.
InUdpSetupTotal / OutUdpSetupTotal	Number of UDP connections in inbound and outbound directions.
InUdpTearTotal / OutUdpTearTotal	Number of deleted UDP connections in inbound and outbound directions.
InIcmpSetupTotal / OutIcmpSetupTotal	Number of ICMP connections in inbound and outbound directions.
InIcmpTearTotal / OutIcmpTearTotal	Number of deleted ICMP connections in inbound and outbound directions.

Related Topics

19.8.73 statistics connect-number zone
19.8.75 statistics zone enable

 Copyright © Huawei Technologies Co., Ltd.

19.8.16 display firewall statistics zone-ip

Function

The **display firewall statistics zone-ip** command displays the status of traffic monitoring function and session thresholds for each protocol.

Format

display firewall statistics zone-ip *zone-name*

Parameters

Parameter	Description	Value
zone-name	Indicates the name of a zone.	The value must be the name of an existing zone.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the traffic monitoring function is enabled and the session thresholds of each protocol are set, you can run the **display firewall statistics zone-ip** command to view the traffic monitoring information of the zone.

Example

Display the configuration of traffic monitoring in zone2.

```
<Huawei> display firewall statistics zone-ip zone2
------------------------------------------------------------------------
              Zone statistics config information
------------------------------------------------------------------------
Zone in enable          0             <enable : 1  disable : 0>
---------------------------------High----------------------Low-------
Tcp connect-number              16384                  12288

Udp connect-number              16384                  12288

Icmp connect-number             16384                  12288

------------------------------------------------------------------------
Zone out enable         0             <enable : 1  disable : 0>
------------------------------------------------------------------------
Tcp connect-number              16384                  12288

Udp connect-number              16384                  12288
```

 Copyright © Huawei Technologies Co., Ltd.

```
Icmp connect-number            16384                12288

------------------------------------------------------------------------------
Ip in enable          0          <enable : 1  disable : 0>
------------------------------------------------------------------------------
Tcp connect-number             16384                12288

Udp connect-number             16384                12288

Icmp connect-number            16384                12288

------------------------------------------------------------------------------
Ip out enable         0          <enable : 1  disable : 0>
------------------------------------------------------------------------------
Tcp connect-number             16384                12288

Udp connect-number             16384                12288

Icmp connect-number            16384                12288

------------------------------------------------------------------------------
```

Related Topics

19.8.72 statistics connect-number ip
19.8.74 statistics ip enable

19.8.17 display firewall whitelist

Function

The **display firewall whitelist** command displays entries in the whitelist.

Format

display firewall whitelist { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **vpn-instance** *vpn-instance-name* }

Parameters

Parameter	Description	Value
all	Displays all the entries in the whitelist.	-
ip-address	Displays the whitelist entry matching the specified IP address.	The value is a valid IPv4 IP address 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 of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all the whitelist entries on the device.

```
<Huawei> display firewall whitelist all
Firewall whitelist items  :
------------------------------------------------------------------------------
IP-Address      Expire-Time(m)  VPN-Instance
------------------------------------------------------------------------------
10.1.1.1        3               vpn1
10.1.1.2        Permanent       vpn2
10.1.1.3        6
 ------------------------------------------------------------------------------
 Total number is : 3
```

Table 19-92 Description of the display firewall whitelist command output

Item	Description
IP-Address	IP address in a whitelist entry.
VPN-Instance	Name of the VPN instance that the IP address in a whitelist entry belongs to.
Expire-Time(m)	Aging time of a whitelist entry, in minutes.
Total number is : 3	There are a total of three entries in the whitelist.

Related Topics

19.8.58 firewall whitelist

19.8.18 display firewall zone

Function

The **display firewall zone** command displays the configuration of a specified zone or all zones.

Format

display firewall zone [*zone-name*] [**interface** | **priority**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
zone-name	Displays the configuration of a specified zone.	The value is a string of 1 to 32 case-sensitive characters. The character string cannot contain name or -.
interface	Displays the interfaces added to the zone.	-
priority	Displays the priorities of all zones.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about all zones configured on the device.

```
<Huawei> display firewall zone
zone zone1
 priority is 5
 interface of the zone is (total number 1):
 Vlanif77

 total number is : 1
```

Table 19-93 Description of the display firewall interzone command output

Item	Description
zone zone1	Security zone named **zone1**. To configure a security zone, run the **firewall zone** command.
priority is 5	Priority of a security zone: 5. To configure the priority for a security zone, run the **priority** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
interface of the zone is (total number 1): Vlanif77	One interface, VLANIF 77, has been added to the zone. To add interfaces a zone, run the **zone** command.
total number is : 1	There is a total of one zone on the device.

Related Topics

19.8.59 firewall zone
19.8.65 priority (security zone view)
19.8.76 zone

19.8.19 display firewall-nat session aging-time

Function

The **display firewall-nat session aging-time** command displays the timeout interval of entries in the firewall session table or NAT session table.

Format

display firewall-nat session aging-time

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the timeout interval of sessions on the firewall session table or NAT session table.

Example

Display the timeout time of all entries in the session table.

```
<Huawei> display firewall-nat session aging-time
-----------------------------------------------
Protocol timeout:
  tcp protocol timeout        : 600   (s)
  tcp-proxy timeout           : 10    (s)
```

 Copyright © Huawei Technologies Co., Ltd.

```
  http protocol timeout        : 120   (s)
  udp protocol timeout         : 120   (s)
  icmp protocol timeout        : 20    (s)
  dns protocol timeout         : 120   (s)
  ftp protocol timeout         : 120   (s)
  ftp-data protocol timeout    : 120   (s)
  rtsp protocol timeout        : 60    (s)
  rtsp-media protocol timeout  : 120   (s)
  sip protocol timeout         : 1800  (s)
  sip-media protocol timeout   : 120   (s)
User-define port timeout:
  tcp protocol port 10001     : 65535 (s)
  tcp protocol port 1         : 111   (s)
  tcp protocol port 4443      : 65535 (s)
  tcp protocol port 181       : 180   (s)
  udp protocol port 180       : 180   (s)
  udp protocol port 182       : 208   (s)
---------------------------------------------
```

Table 19-94 Description of the **display firewall-nat session aging-time** command output

Item	Description
Protocol timeout	Session timeout interval of each protocol.
tcp protocol timeout	Timeout interval of TCP connections. The default value is 600, in seconds.
tcp-proxy timeout	Timeout interval of the TCP proxy. The default value is 10, in seconds.
udp protocol timeout	Timeout interval of UDP connections. The default value is 120, in seconds.
icmp protocol timeout	Timeout interval of ICMP connections. The default value is 20, in seconds.
dns protocol timeout	Timeout interval of the DNS protocol. The default value is 120, in seconds.
http protocol timeout	Timeout interval of the HTTP connections. The default value is 120, in seconds.
ftp protocol timeout	Timeout interval of the FTP control connection. The default value is 120, in seconds.
ftp-data protocol timeout	Timeout interval of the FTP connections. The default value is 120, in seconds.
sip protocol timeout	Timeout interval of the SIP protocol. The default value is 1800, in seconds.
sip-media protocol timeout	Timeout interval of the SIP media protocol. The default value is 120, in seconds.
rtsp protocol timeout	Timeout interval of the RTSP protocol. The default value is 60, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
rtsp-media protocol timeout	Timeout interval of the RTSP media protocol. The default value is 120, in seconds.
User-define port timeout	Timeout interval of a connection with a user-defined port as the destination port.
tcp protocol port *port-number*	Timeout interval of a data connection with a user-defined TCP port as the destination port. The default value is the default data connection timeout interval of the corresponding protocol, in seconds.
udp protocol port *port-number*	Timeout interval of a data connection with a user-defined UDP port as the destination port. The default value is the default data connection timeout interval of the corresponding protocol, in seconds.

Related Topics

19.8.60 firewall-nat session aging-time

19.8.20 display port-mapping

Function

The **display port-mapping** command displays mappings between the specified application-layer protocols and ports.

Format

display port-mapping [**dns** | **ftp** | **http** | **rtsp** | **sip** | **port** *port-number* | **pptp**]

Parameters

Parameter	Description	Value
dns	Displays the mapping between the DNS protocol and port.	-
ftp	Displays the mapping between the FTP protocol and port.	-
http	Displays the mapping between the HTTP protocol and port.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rtsp	Displays the mapping between the RTSP protocol and port.	-
sip	Displays the mapping between the SIP protocol and port.	-
port *port-number*	Displays the mapping between the specified port and the application-layer protocol.	The value is an integer that ranges from 1 to 65535.
pptp	Displays the mapping between the PPTP protocol and port.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display port-mapping** command displays the port mappings, including the mappings between application-layer protocols and ports, condition (ACL) in which each mapping takes effect, and the type of each mapping (defined by the system or user).

Example

Display the mapping between the DNS protocol and port.

```
<Huawei> display port-mapping dns
 ------------------------------------------------
 Service    Port       Acl        Type
 ------------------------------------------------
 dns        53                    system defined
 ------------------------------------------------
Total number is : 1
```

Table 19-95 Description of the display port-mapping command output

Item	Description
Service	Type of the application-layer protocol.
Port	Port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Acl	Number of the ACL for mappings.
Type	Mapping type. • system defined: default mapping. • user defined: mapping defined by the user.
Total number is : 1	The total number of mappings is 1.

Related Topics

19.8.64 port-mapping

19.8.21 display session

Function

The **display session** command displays the session table information.

Format

display session { **all** [**verbose**] | **number** }

display session destination *destination-address* [*destination-port*] [**verbose**]

display session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all session table information.	-
verbose	Displays detailed information about the session table.	-
number	Displays the number of entries in the session table.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol { *protocol-number* | *protocol-name* }	Displays entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMP, TCP, or UDP.
source *source-address* [*source-port*]	Displays entries with a specified source IP address or both a source IP address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• *source-address* is in dotted decimal notation. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Displays entries with a specified destination IP address or both a destination IP address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• *destination-address* is in dotted decimal notation. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about a firewall session table, NAT session table, or a common session table.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the number of entries in the session table.

```
<Huawei> display session number
 The total number of session tables is: 1
```

Display details about all entries in the session table.

```
<Huawei> display session all verbose
  Session Table Information:
    Protocol          : TCP(6)
    SrcAddr  Port Vpn : 10.200.200.200 65532 vpn1
    DestAddr Port Vpn : 10.100.100.100 1024
    Time To Live      : 60 s
    NAT-Info
      New SrcAddr     : 10.10.10.10
      New SrcPort     : 10240
      New DestAddr    : 10.30.30.30
      New DestPort    : 21
    Firewall-Info
      InZone          : a
      OutZone         : b

  Total : 1
```

Table 19-96 Description of the display session all verbose command output

Item	Description
Protocol	Protocol type.
SrcAddr Port Vpn	Source address, service port number, and VPN instance name.
DestAddr Port Vpn	Destination address, service port number, and VPN instance name.
Time To Live	Lifetime of the session table entries.
NAT-Info	NAT information.
New SrcAddr	Translated source IP address.
New SrcPort	Translated source port.
New DestAddr	Translated destination IP address.
New DestPort	Translated destination port.
Firewall-Info	Firewall information.
InZone	Inbound zone name.
OutZone	Outbound zone name.
Total	Number of entries in the session table.

 Copyright © Huawei Technologies Co., Ltd.

19.8.22 firewall blacklist

Function

The **firewall blacklist** command adds an entry to the blacklist.

The **undo firewall blacklist** command deletes an entry from the blacklist.

Format

firewall blacklist *ip-address* [**vpn-instance** *vpn-instance-name*] [**expire-time** *minutes*]

undo firewall blacklist { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **vpn-instance** *vpn-instance-name* }

Parameters

Parameter	Description	Value
ip-address	Indicates the IP address that you want to add to the blacklist.	The value is a valid IPv4 IP address.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.
expire-time *minutes*	Specifies the aging time of a blacklist entry.	The value is an integer that ranges from 1 to 1000, in minutes. **NOTE** If this parameter is not set, the entry is always valid.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After an IP address is added to the blacklist by the **firewall blacklist** command, the firewall denies the packets from this IP address until this entry ages.

An IP address cannot exist in both the whitelist and blacklist.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The blacklist entry with an aging time is not written into the configuration file. You can view it using the **19.8.7 display firewall blacklist** command.

Example

Add IP address 192.168.10.10 to the blacklist entry and set its aging time to 100 minutes.

```
<Huawei> system-view
[Huawei] firewall blacklist 192.168.10.10 expire-time 100
```

Related Topics

19.8.7 display firewall blacklist

19.8.23 firewall blacklist enable

Function

The **firewall blacklist enable** command enables the blacklist function.

The **undo firewall blacklist enable** command disables the blacklist function.

By default, the blacklist function is disabled.

Format

firewall blacklist enable

undo firewall blacklist enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configurations of the blacklist take effect only after you run the **firewall blacklist enable** command to enable the blacklist function.

Precautions

A blacklist entry can be manually configured or automatically generated.

 Copyright © Huawei Technologies Co., Ltd.

After you run the **firewall defend ip-sweep enable** command to enable defense against address scanning attacks, the device adds attacking IP addresses to the blacklist.

After you run the **firewall defend port-scan enable** command to enable defense against port scanning attacks, the device adds attacking ports to the blacklist.

Example

Enable the blacklist function.

```
<Huawei> system-view
[Huawei] firewall blacklist enable
```

19.8.24 firewall black-white-list load configuration-file

Function

The **firewall black-white-list load configuration-file** command loads the configuration file of blacklist and whitelist.

Format

firewall black-white-list load configuration-file *configuration-file-name*

Parameters

Parameter	Description	Value
configuration-file-name	Indicates the name of the configuration file.	The value is a string of 1 to 127 characters in the format [drive][file-name] (the default drive is flash:/). The configuration file is in txt format.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can batch configure entries in the blacklist and whitelist by loading a configuration file.

A configuration file can contain multiple entries, but the entries must be edited one by one. Blank lines are allowed between lines. A configuration file contains up to 50000 lines. The following is an example of the configuration file:

 Copyright © Huawei Technologies Co., Ltd.

```
[FirewallBlacklist]
IPAddress = 10.10.10.1
VPNName = vpna
[FirewallBlacklist]
IPAddress = 10.10.10.2
VPNName =

[FirewallWhitelist]
IPAddress = 10.10.10.3
VPNName = vpnb
[FirewallWhitelist]
IPAddress = 10.20.20.1
VPNName =
```

NOTE

An invalid configuration file cannot be loaded. For example, if a configuration file contains an invalid IP address or excess entries, the invalid IP address cannot be added and the excess entries do not take effect; however, the valid IP addresses and the entries in the range can still take effect.

Example

Load the configuration file named **bwls.txt**.

```
<Huawei> system-view
[Huawei] firewall black-white-list load configuration-file bwls.txt
```

Related Topics

19.8.25 firewall black-white-list save configuration-file

19.8.25 firewall black-white-list save configuration-file

Function

The **firewall black-white-list save configuration-file** command saves the blacklist and whitelist to a configuration file.

Format

firewall black-white-list save configuration-file *configuration-file-name*

Parameters

Parameter	Description	Value
configuration-file-name	Indicates the name of the configuration file.	The value is a string of 1 to 127 characters in the format [drive][file-name] (the default drive is flash:/). The configuration file is in txt format.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By using this command, you can save the blacklist and whitelist to the configuration file *configuration-file-name*. Only the entries with the aging time being 0 can be saved.

NOTE

The configuration file *configuration-file-name* must be available before this command is executed.

Example

Save the blacklist and whitelist to the configuration file **bls_wls.txt**.

```
<Huawei> system-view
[Huawei] firewall black-white-list save configuration-file bwls.txt
```

Related Topics

19.8.24 firewall black-white-list load configuration-file

19.8.26 firewall defend all enable

Function

The **firewall defend all enable** command enables all the attack defense functions.

The **undo firewall defend all enable** command disables all the attack defense functions.

By default, no attack defense function is enabled.

Format

firewall defend all enable

undo firewall defend all enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable all attack defense functions.

```
<Huawei> system-view
[Huawei] firewall defend all enable
```

Related Topics

19.8.9 display firewall defend

19.8.27 firewall defend fraggle enable

Function

The **firewall defend fraggle enable** command enables the Fraggle attack defense function.

The **undo firewall defend fraggle enable** command disables the Fraggle attack defense function.

By default, the Fraggle attack defense function is disabled.

Format

firewall defend fraggle enable

undo firewall defend fraggle enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A Fraggle attack is similar to a Smurf attack, except that the Fraggle attack sends UDP packets, rather than ICMP packets. Therefore, the Fraggle attack packets can traverse some firewalls that prevent ICMP packets.

 Copyright © Huawei Technologies Co., Ltd.

A Fraggle attack can be successful because both UDP port 7 (ECHO) and port 19 (Chargen) return responses after receiving UDP packets. The details are as follows:

- UDP port 7 returns a response (similar to the ICMP ECHO-Reply packet) after receiving a packet.
- UDP port 19 generates a character stream after receiving the packet.

The two UDP ports send a lot of response packets, which occupy high network bandwidth.

An attacker can send a UDP packet to the target network. The source address of the UDP packet is the IP address of the attacked host and its destination address is the broadcast address or network address of the host's subnet. The destination port number of the packet is 7 or 19. All the hosts on the subnet then send response packets to the attacked host. This generates heavy traffic and hence congests the network or makes the host break down.

Example

Enable the Fraggle attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend fraggle enable
```

Related Topics

19.8.9 display firewall defend

19.8.28 firewall defend icmp-flood

Function

The **firewall defend icmp-flood** command sets the parameters of ICMP Flood attack defense, including the protected zone or IP address and maximum connection rate.

The **undo firewall defend icmp-flood** command restores the default values of ICMP Flood attack defense parameters.

By default, the maximum connection rate of ICMP Flood attack defense is 1000 pps.

Format

firewall defend icmp-flood { **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **zone** *zone-name* } [**max-rate** *rate-value*]

undo firewall defend icmp-flood [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies a protected IP address.	The value is a valid IPv4 IP address.
zone *zone-name*	Specifies a protected zone.	The value of *zone-name* is a string of 1 to 32 characters. It must be an existing zone name.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.
max-rate *rate-value*	Specifies the maximum connection rate of a new flow.	The value of *rate-value* is an integer that ranges from 1 to 65535, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ICMP Flood attack sends a large number of ICMP packets (such as ping packets) to the attacked host in a short time and requests for responses. The host is then overloaded and cannot process normal tasks.

ICMP Flood attack defense parameters configured for an IP address take precedence over those configured for a zone. If ICMP Flood attack defense is configured for both an IP address and the zone where the IP address resides, the configuration for the IP address takes effect. If you cancel the configuration for the IP address, the configuration for the zone takes effect.

Precautions

Parameters of ICMP Flood attack defense take effect only after ICMP Flood defense is enabled using the **firewall defend icmp-flood enable** command.

Example

Enable ICMP Flood attack defense for IP address 10.1.64.200 and set the maximum connection rate of ICMP packets to 500 pps.

```
<Huawei> system-view
[Huawei] firewall defend icmp-flood enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] firewall defend icmp-flood ip 10.1.64.200 max-rate 500
```

Related Topics

19.8.9 display firewall defend

19.8.27 firewall defend fraggle enable

19.8.29 firewall defend icmp-flood enable

Function

The **firewall defend icmp-flood enable** command enables the ICMP Flood attack defense function.

The **undo firewall defend icmp-flood enable** command disables the ICMP Flood attack defense function.

By default, the ICMP Flood attack defense function is disabled.

Format

firewall defend icmp-flood enable

undo firewall defend icmp-flood enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ICMP Flood attack sends a large number of ICMP packets (such as ping packets) to the attacked host in a short time and requests for responses. The host is then overloaded and cannot process normal tasks.

Precaution

You can run **firewall defend icmp-flood** command to set parameters for ICMP Flood attack defense.

Example

Enable the ICMP Flood attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend icmp-flood enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.8.9 display firewall defend
19.8.28 firewall defend icmp-flood

19.8.30 firewall defend icmp-redirect enable

Function

The **firewall defend icmp-redirect enable** command enables the ICMP-Redirect attack defense function.

The **undo firewall defend icmp-redirect enable** command disables the ICMP-Redirect attack defense function.

By default, the ICMP-Redirect attack defense function is disabled.

Format

firewall defend icmp-redirect enable

undo firewall defend icmp-redirect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the ICMP-Redirect attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend icmp-redirect enable
```

Related Topics

19.8.9 display firewall defend

 Copyright © Huawei Technologies Co., Ltd.

19.8.31 firewall defend icmp-unreachable enable

Function

The **firewall defend icmp-unreachable enable** command enables the ICMP-Unreachable attack defense function.

The **undo firewall defend icmp-unreachable enable** command disables the ICMP-Unreachable attack defense function.

By default, the ICMP-Unreachable attack defense function is disabled.

Format

firewall defend icmp-unreachable enable

undo firewall defend icmp-unreachable enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the ICMP-Unreachable attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend icmp-unreachable enable
```

Related Topics

19.8.9 display firewall defend

19.8.32 firewall defend ip-fragment enable

Function

The **firewall defend ip-fragment enable** command enables the IP fragment attack defense function.

The **undo firewall defend ip-fragment enable** command disables the IP fragment attack defense function.

 Copyright © Huawei Technologies Co., Ltd.

By default, the IP fragment attack defense function is disabled.

Format

firewall defend ip-fragment enable

undo firewall defend ip-fragment enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable the IP fragment attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend ip-fragment enable
```

Related Topics

19.8.9 display firewall defend

19.8.33 firewall defend ip-sweep

Function

The **firewall defend ip-sweep** command sets the parameters of address sweeping attack defense, including the maximum session rate and blacklist timeout interval.

The **undo firewall defend ip-sweep** command restores the default values of address sweeping attack defense parameters.

By default, the maximum session rate for address scanning and port scanning attack defense is 4000 pps, and the blacklist timeout interval is 20 minutes.

Format

firewall defend ip-sweep { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }

undo firewall defend ip-sweep { **blacklist-expire-time** | **max-rate** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
blacklist-expire-time *interval*	Specifies the timeout interval of blacklist entries. After an IP address stays in the blacklist for the specified period, the firewall deletes the IP address from the blacklist. Then the IP address can initiate connections.	The value of *interval* is an integer that from 1 to 1000, in minutes. The default value is 20.
max-rate *rate-value*	Specifies the maximum session rate. When the session rate of an IP address exceeds the limit, the firewall considers that an IP address sweeping attack occurs. Then the firewall adds the IP address to the blacklist and denies the new sessions from the IP address or port.	The value of *rate-value* is an integer that ranges from 1 to 10000, in pps. The default value is 4000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Parameters of address sweeping attack defense take effect only after address sweeping attack defense is enabled using the **firewall defend ip-sweep enable** command.

Example

Enable the address sweeping attack defense function, set the maximum session rate to 1000 pps, and set the blacklist timeout interval to 5 minutes.

```
<Huawei> system-view
[Huawei] firewall defend ip-sweep enable
[Huawei] firewall defend ip-sweep max-rate 1000
[Huawei] firewall defend ip-sweep blacklist-expire-time 5
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.8.9 display firewall defend

19.8.34 firewall defend ip-sweep enable

19.8.34 firewall defend ip-sweep enable

Function

The **firewall defend ip-sweep enable** command enables the IP sweeping attack defense function.

The **undo firewall defend ip-sweep enable** command disables the IP sweeping attack defense function.

By default, the IP sweeping attack defense function is disabled.

Format

firewall defend ip-sweep enable

undo firewall defend ip-sweep enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP sweeping attack detects the IP addresses of the target hosts by using scanning tools. The attacker then determines the hosts that exist on the target network according to the responses received.

Precaution

You can run **firewall defend ip-sweep** command to set parameters for IP address sweep attack defense.

Example

Enable the IP sweeping defense function.

```
<Huawei> system-view
[Huawei] firewall defend ip-sweep enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.8.9 display firewall defend
19.8.33 firewall defend ip-sweep

19.8.35 firewall defend land enable

Function

The **firewall defend land enable** command enables the defense against Land attacks.

The **undo firewall defend land enable** command disables the defense against Land attacks.

By default, the Land attack defense function is disabled.

Format

firewall defend land enable

undo firewall defend land enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable the defense against Land attacks.

```
<Huawei> system-view
[Huawei] firewall defend land enable
```

Related Topics

19.8.9 display firewall defend

 Copyright © Huawei Technologies Co., Ltd.

19.8.36 firewall defend large-icmp

Function

The **firewall defend large-icmp** command sets the maximum length of ICMP packets allowed to pass.

The **undo firewall defend large-icmp** command restores the default maximum length of ICMP packets allowed to pass.

By default, the maximum length of ICMP packet allowed to pass is 4000 bytes.

Format

firewall defend large-icmp max-length *length*

undo firewall defend large-icmp max-length

Parameters

Parameter	Description	Value
max-length *length*	Specifies the maximum length of ICMP packets allowed to pass.	The value of *length* is an integer that ranges from 28 to 65535, in bytes. The default value is 4000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Similar to a "Ping of Death" attack, a Large-ICMP attack sends the oversized ICMP packets to attack a system. The difference is that the length of Large-ICMP packet does not exceed the maximum length of an IP packet (65535 bytes). Large-ICMP packets also have great impact on some operating systems. To prevent Large-ICMP attack, set the maximum length of ICMP packets on the firewall.

Precautions

The maximum length of ICMP packets allowed to pass takes effect only after large-ICMP attack defense is enabled using the **firewall defend large-icmp enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable Large-ICMP attack defense and set the maximum length of ICMP packet allowed to pass to 4000 bytes.

```
<Huawei> system-view
[Huawei] firewall defend large-icmp enable
[Huawei] firewall defend large-icmp max-length 4000
```

Related Topics

19.8.9 display firewall defend

19.8.37 firewall defend large-icmp enable

Function

The **firewall defend large-icmp enable** command enables the Large-ICMP attack defense function.

The **undo firewall defend large-icmp enable** command disables the Large-ICMP attack defense function.

By default, the Large-ICMP attack defense function is disabled.

Format

firewall defend large-icmp enable

undo firewall defend large-icmp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Similar to a "Ping of Death" attack, a large-ICMP attack sends the oversize ICMP packets to attack a system. The difference is that the length of Large-ICMP packet does not exceed the maximum length of an IP packet (65535 bytes). Large-ICMP packets also have great impact on some operating systems.

Precaution

You can run **firewall defend large-icmp** command to set Large-ICMP attack defense.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the Large-ICMP attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend large-icmp enable
```

Related Topics

19.8.9 display firewall defend

19.8.36 firewall defend large-icmp

19.8.38 firewall defend ping-of-death enable

Function

The **firewall defend ping-of-death enable** command enables the defense against Ping of Death attack.

The **undo firewall defend ping-of-death enable** command disables the defense against Ping of Death attack.

By default, the defense against Ping of Death attack is disabled.

Format

firewall defend ping-of-death enable

undo firewall defend ping-of-death enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the defense against Ping of Death attack.

```
<Huawei> system-view
[Huawei] firewall defend ping-of-death enable
```

Related Topics

19.8.9 display firewall defend

 Copyright © Huawei Technologies Co., Ltd.

19.8.39 firewall defend port-scan

Function

The **firewall defend port-scan** command sets the parameters of port scanning attack defense, including the maximum session rate and blacklist timeout interval.

The **undo firewall defend port-scan** command restores the default values of port scanning attack defense parameters.

By default, the maximum session rate for port scanning attack defense is 4000 pps, and the blacklist timeout interval is 20 minutes.

Format

firewall defend port-scan { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }

undo firewall defend port-scan { **blacklist-expire-time** | **max-rate** }

Parameters

Parameter	Description	Value
blacklist-expire-time *interval*	Specifies the timeout interval of blacklist entries. After a port stays in the blacklist for the specified period, the firewall deletes the port from the blacklist. Then the port can initiate connections.	The value of *interval* is an integer that from 1 to 1000, in minutes. The default value is 20.
max-rate *rate-value*	Specifies the maximum session rate. When the session rate of a port exceeds the limit, the firewall considers that a scanning attack occurs. Then the firewall adds the port to the blacklist and denies the new sessions from the port.	The value of *rate-value* is an integer that ranges from 1 to 10000, in pps. The default value is 4000.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Parameters of port scanning attack defense take effect only after port scanning attack defense is enabled using the **firewall defend port-scan enable** command.

Example

Enable the port scanning attack defense function, set the maximum session rate to 1000 pps, and set the blacklist timeout interval to 5 minutes.

```
<Huawei> system-view
[Huawei] firewall defend port-scan enable
[Huawei] firewall defend port-scan max-rate 1000
[Huawei] firewall defend port-scan blacklist-expire-time 5
```

Related Topics

19.8.9 display firewall defend

19.8.40 firewall defend port-scan enable

19.8.40 firewall defend port-scan enable

Function

The **firewall defend port-scan enable** command enables the port scanning attack defense function.

The **undo firewall defend port-scan enable** command disables the port scanning attack defense function.

By default, the port scanning attack defense function is disabled.

Format

firewall defend port-scan enable

undo firewall defend port-scan enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

Port scanning attack detects the ports of the target hosts by using scanning tools. The attacker then finds out the hosts that exist on the target network according to the responses and the ports that are used to provide services.

Precaution

You can run the **firewall defend port-scan** command to set parameters for port scanning attack defense.

Example

Enable the port scanning attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend port-scan enable
```

Related Topics

19.8.9 display firewall defend

19.8.39 firewall defend port-scan

19.8.41 firewall defend smurf enable

Function

The **firewall defend smurf enable** command enables the Smurf attack defense function.

The **undo firewall defend smurf enable** command disables the Smurf attack defense function.

By default, the Smurf attack defense function is disabled.

Format

firewall defend smurf enable

undo firewall defend smurf enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Enables the Smurf attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend smurf enable
```

Related Topics

19.8.9 display firewall defend

19.8.42 firewall defend syn-flood

Function

The **firewall defend syn-flood** command sets the parameters of SYN Flood attack defense, including the protected zone or IP address and maximum connection rate.

The **undo firewall defend syn-flood** command restores the default configuration of SYN Flood attack defense.

By default, the maximum connection rate of SYN Flood attack defense is 1000 pps.

Format

firewall defend syn-flood { **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **zone** *zone-name* } [**max-rate** *rate-value*] [**tcp-proxy** { **auto** | **off** | **on** }]

undo firewall defend syn-flood [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]]

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies a protected IP address.	The value is a valid IPv4 IP address.
zone *zone-name*	Specifies a protected zone.	The value of *zone-name* is a string of 1 to 32 characters. It must be an existing zone name.
max-rate *rate-value*	Specifies the maximum connection rate of a new flow.	The value of *rate-value* is an integer that ranges from 1 to 65535. The default value is 1000, in pps.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tcp-proxy { **auto** | **off** | **on** }	Indicates whether to use the TCP proxy. The status of TCP proxy includes: • **auto**: The TCP proxy is enabled automatically when the actual connection rate exceeds the upper limit. • **off**: The TCP proxy is always disabled. • **on**: The TCP proxy is always enabled.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flood attack defense parameters configured for an IP address take precedence over those configured for a zone. If Flood attack defense is configured for both an IP address and the zone where the IP address resides, the configuration for the IP address takes effect. If you cancel the configuration for the IP address, the configuration for the zone takes effect.

Precautions

Parameters of SYN Flood attack defense take effect only after SYN Flood attack defense is enabled using the **firewall defend syn-flood enable** command.

Example

Enable SYN Flood attack defense for IP address 10.1.64.200 and set the maximum connection rate of TCP packets to 500 pps.

```
<Huawei> system-view
[Huawei] firewall defend syn-flood enable
[Huawei] firewall defend syn-flood ip 10.1.64.200 max-rate 500
```

Related Topics

19.8.9 display firewall defend

19.8.43 firewall defend syn-flood enable

 Copyright © Huawei Technologies Co., Ltd.

19.8.43 firewall defend syn-flood enable

Function

The **firewall defend syn-flood enable** command enables the SYN Flood attack defense function.

The **undo firewall defend syn-flood enable** command disables the SYN Flood attack defense function.

By default, the SYN Flood attack defense function is disabled.

Format

firewall defend syn-flood enable

undo firewall defend syn-flood enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The TCP/IP protocol stack permits only a certain number of TCP connections due to resource restriction. SYN Flood attacks utilize this feature. The attacker forges a SYN packet with a forged or nonexistent source address to initiate a connection to the server. When receiving this packet, the server replies with a SYN-ACK message. The receiver of the SYN-ACK packet does not exist, so a half-connection is caused. If the attacker sends a large number of such packets, a lot of half-connections will be produced on the attacked host and the resources of the attacked host will be exhausted. Therefore, authorized users cannot access the host till the half-connections expire. If the number of connections is not limited, SYN Flood will consume the system resources such as memory.

Precaution

You can run **firewall defend syn-flood** command to set parameters for SYN Flood attack defense.

Example

Enable the SYN Flood attack defense function.

```
<Huawei> system-view
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] firewall defend syn-flood enable
```

Related Topics

19.8.9 display firewall defend

19.8.28 firewall defend icmp-flood

19.8.44 firewall defend tcp-flag enable

Function

The **firewall defend tcp-flag enable** command enables the defense against TCP flag attack.

The **undo firewall defend tcp-flag enable** command disables the defense against TCP flag attack.

By default, the TCP flag attack defense function is disabled.

Format

firewall defend tcp-flag enable

undo firewall defend tcp-flag enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the TCP flag attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend tcp-flag enable
```

Related Topics

19.8.9 display firewall defend

 Copyright © Huawei Technologies Co., Ltd.

19.8.45 firewall defend teardrop enable

Function

The **firewall defend teardrop enable** command enables the defense against Teardrop attack.

The **undo firewall defend teardrop enable** command disables the defense against Teardrop attack.

By default, the Teardrop attack defense function is disabled.

Format

firewall defend teardrop enable

undo firewall defend teardrop enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable the defense against Teardrop attack.

```
<Huawei> system-view
[Huawei] firewall defend teardrop enable
```

Related Topics

19.8.9 display firewall defend

19.8.46 firewall defend tracert enable

Function

The **firewall defend tracert enable** command enables the Tracert attack defense function.

The **undo firewall defend tracert enable** command disables the Tracert attack defense function.

 Copyright © Huawei Technologies Co., Ltd.

By default, the Tracert attack defense function is disabled.

Format

firewall defend tracert enable

undo firewall defend tracert enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Tracert attack traces the path of an ICMP timeout packet returned when the value of time to live (TTL) is 0 or an ICMP port-unreachable packet. In this way, the attacker obtains the network structure.

Example

Enable the Tracert attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend tracert enable
```

Related Topics

19.8.9 display firewall defend

19.8.47 firewall defend udp-flood

Function

The **firewall defend udp-flood** command sets the parameters of UDP Flood attack defense, including the protected zone or IP address and maximum connection rate.

The **undo firewall defend udp-flood** command restores the default configuration of UDP Flood attack defense.

By default, the maximum connection rate of UDP Flood attack defense is 1000 pps.

Format

firewall defend udp-flood { **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **zone** *zone-name* } [**max-rate** *rate-value*]

 Copyright © Huawei Technologies Co., Ltd.

undo firewall defend udp-flood [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]]

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies a protected IP address.	The value is a valid IPv4 IP address.
zone *zone-name*	Specifies a protected zone.	The value of *zone-name* is a string of 1 to 32 characters. It must be an existing zone name.
max-rate *rate-value*	Specifies the maximum connection rate of a new flow.	The value of *rate-value* is an integer that ranges from 1 to 65535. The default value is 1000, in pps.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

UDP Flood attack sends a large number of UDP packets to the attacked host in a short time and requests for responses. The host is then overloaded and cannot process normal tasks.

Flood attack defense parameters configured for an IP address take precedence over those configured for a zone. If Flood attack defense is configured for both an IP address and the zone where the IP address resides, the configuration for the IP address takes effect. If you cancel the configuration for the IP address, the configuration for the zone takes effect.

Precautions

Parameters of UDP Flood attack defense take effect only after UDP Flood attack defense is enabled using the **firewall defend udp-flood enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable UDP Flood attack defense for IP address 10.1.64.200 and set the maximum connection rate of UDP packets to 500 pps.

```
<Huawei> system-view
[Huawei] firewall defend udp-flood enable
[Huawei] firewall defend udp-flood ip 10.1.64.200 max-rate 500
```

Related Topics

19.8.9 display firewall defend

19.8.48 firewall defend udp-flood enable

Function

The **firewall defend udp-flood enable** command enables the UDP Flood attack defense function.

The **undo firewall defend udp-flood enable** command disables the UDP Flood attack defense function.

By default, the UDP Flood attack defense function is disabled.

Format

firewall defend udp-flood enable

undo firewall defend udp-flood enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

UDP Flood attack sends a large number of UDP packets to the attacked host in a short time and requests for responses. The host is then overloaded and cannot process normal tasks.

Precaution

You can run **firewall defend udp-flood** command to set parameters for ICMP Flood attack defense.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable UDP Flood attack defense.

```
<Huawei> system-view
[Huawei] firewall defend udp-flood enable
```

Related Topics

19.8.9 display firewall defend

19.8.49 firewall defend winnuke enable

Function

The **firewall defend winnuke enable** command enables the WinNuke attack defense function.

The **undo firewall defend winnuke enable** command disables the WinNuke attack defense function.

By default, the WinNuke attack defense function is disabled.

Format

firewall defend winnuke enable

undo firewall defend winnuke enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

WinNuke attack sends an out-of-band (OOB) data packet to the NetBIOS port (139) of the target host running a Windows operating system. The NetBIOS fragment then overlaps and the host stops responding. An Internet Group Management Protocol (IGMP) fragment packet can also damage the target host because the IGMP packet should not be fragmented. If a host receives an IGMP fragment packet, the host may be attacked.

Example

Enables the WinNuke attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend winnuke enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.8.9 display firewall defend

19.8.50 firewall enable

Function

The **firewall enable** command enables the firewall function in an interzone.

The **undo firewall enable** command disables the firewall function in an interzone.

By default, the firewall function is disabled in an interzone.

Format

firewall enable

undo firewall enable

Parameters

None

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

The packet filtering, ASPF, and attack defense functions take effect only after this command is executed. This command does not needs to be executed for other advanced security features, such as IPS and URL filtering.

Example

Enable the firewall function in the interzone between zone1 and zone2.

```
<Huawei> system-view
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] firewall enable
```

Related Topics

19.8.10 display firewall interzone

19.8.51 firewall interzone

Function

The **firewall interzone** command creates an interzone.

 Copyright © Huawei Technologies Co., Ltd.

The **undo firewall interzone** command deletes an interzone.

Format

firewall interzone *zone-name1 zone-name2*

undo firewall interzone *zone-name1 zone-name2*

Parameters

Parameter	Description	Value
zone-name1	Specifies the name of a zone included in the interzone.	The name is a string of 1 to 32 characters. *zone-name1* must be a zone name created by the **19.8.59 firewall zone** command.
zone-name2	Specifies the name of the other zone included in the interzone.	The name is a string of 1 to 32 characters. *zone-name2* must be a zone name created by the **19.8.59 firewall zone** command.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the firewall in an interzone to filter packets or application-layer services, run the **firewall interzone** command to enter the interzone view.

Precautions

At least two valid zones must exist on the device; otherwise, the device does not execute the **firewall interzone** command.

The interzone is determined by two zones, which is irrelevant to the sequence of the two zones in the command.

Example

Create an interzone between zone1 and zone2.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] firewall interzone zone1 zone2
```

Related Topics

19.8.10 display firewall interzone

19.8.52 firewall log binary-log host

Function

The **firewall log binary-log host** command sets parameters of a binary log server, including the IP address and port number of the binary log server, and the IP address and port number that the local device uses to communicate with the log server.

The **undo firewall log binary-log host** command deletes a binary log server.

Format

firewall log binary-log host *host-ip-address host-port* **source** *source-ip-address source-port* [**vpn-instance** *vpn-instance-name*]

undo firewall log binary-log host

Parameters

Parameter	Description	Value
host-ip-address	Specifies the IP address of the log server.	The value is a valid IPv4 IP address.
host-port	Specifies the port number of the log server.	The value is an integer that ranges from 1 to 65535.
source-ip-address	Specifies the source IP address that the local device uses to send logs to the log server.	The value is a valid IPv4 IP address.
source-port	Specifies the source port number that the local device uses to send logs to the log server.	The value is an integer that ranges from 10240 to 55534.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the source IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Only one binary log server can be configured in the system view. Any time a new binary log server is configured, the new one replaces the previous one.

Example

Configure a binary log server whose IP address is 10.10.10.1 and port number is 3456. Set the source IP address and source port number used to communicate with the log server to 10.10.10.2 and 20000 respectively.

```
<Huawei> system-view
[Huawei] firewall log binary-log host 10.10.10.1 3456 source 10.10.10.2 20000
```

Related Topics

19.8.12 display firewall log configuration

19.8.53 firewall log enable

Function

The **firewall log enable** command enables the firewall logging function.

The **undo firewall log enable** command disables the firewall logging function.

By default, firewall logging function is disabled.

Format

firewall log { **all** | **blacklist** | **defend** | **session** | **statistics** | **packet-filter** } **enable**

undo firewall log { **all** | **blacklist** | **defend** | **session** | **statistics** | **packet-filter** } **enable**

Parameters

Parameter	Description	Value
all	Enables all the logging functions on the firewall. **NOTE** Firewall logs are classified into blacklist logs, attack defense logs, session logs, and traffic statistics logs.	-
blacklist	Enables blacklist logs.	-
defend	Enables attack defense logs.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
session	Enables session logs.	-
statistics	Enables traffic statistics logs.	-
packet-filter	Enables packet-filter logs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Firewall logs record the operating status of the firewall in real time. By analyzing the logs, the network administrator can find potential security threats to the network and take preventive measures to protect the network.

You can configure the following types of logs on the firewall:

- Blacklist log: records the IP addresses that are added to or deleted from the blacklist.
- Attack defense log: records different types of attacks detected by the firewall.
- Session log: records the sessions that match the specified ACL rules and sessions processed by the NAT server.
- Traffic statistics log: records the events that the traffic rate exceeds the threshold or falls below the threshold.
- Packet filtering log: records information about packet filtering.

Example

Enable blacklist logs.

```
<Huawei> system-view
[Huawei] firewall log blacklist enable
```

Related Topics

19.8.54 firewall log log-interval

19.8.12 display firewall log configuration

 Copyright © Huawei Technologies Co., Ltd.

19.8.54 firewall log log-interval

Function

The **firewall log log-interval** command sets the interval for exporting firewall logs.

The **undo firewall log log-interval** command restores the default interval for exporting firewall logs.

By default, firewall logs are exported every 30 seconds.

Format

firewall log { **blacklist** | **defend** | **session** | **statistics** | **packet-filter** } **log-interval** *time*

undo firewall log { **blacklist** | **defend** | **session** | **statistics** | **packet-filter** } **log-interval**

Parameters

Parameter	Description	Value
blacklist	Sets the interval for sending blacklist logs to the log server.	-
defend	Sets the interval for sending attack defense logs to the log server.	-
session	Sets the interval for sending session logs to the log server.	-
statistics	Sets the interval for sending traffic statistics logs to the log server.	-
packet-filter	Sets the interval for sending packet filtering logs to the log server.	-
log-interval *time*	Specifies the value of the interval.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Firewall logs are classified into binary logs and text logs depending on the format. Binary logs are sent to the binary log server in real time, and text logs are sent to the text log server at intervals. The **firewall log log-interval** command sets the interval for sending text logs to the text log server.

Example

Set the interval for sending attack defense logs to the log server to 200 seconds.

```
<Huawei> system-view
[Huawei] firewall log defend log-interval 200
```

Related Topics

19.8.53 firewall log enable

19.8.12 display firewall log configuration

19.8.55 firewall log session nat enable

Function

The **firewall log session nat enable** command enables NAT session logs.

The **undo firewall log session nat enable** command disables NAT session logs.

By default, NAT session logs are disabled.

Format

firewall log session nat enable

undo firewall log session nat enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Session logs record the sessions that match the specified ACL rules and sessions processed by the NAT server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable NAT session logs.

```
<Huawei> system-view
[Huawei] firewall log session nat enable
```

Related Topics

19.8.53 firewall log enable

19.8.54 firewall log log-interval

19.8.12 display firewall log configuration

19.8.56 firewall statistics system connect-number

Function

The **firewall statistics system connect-number** command sets the session thresholds on the firewall.

The **undo firewall statistics system connect-number** command restores the default session thresholds on the firewall.

Format

firewall statistics system connect-number { **frag** | **icmp** | **tcp** | **tcp-proxy** | **udp** } **high** *high-threshold* **low** *low-threshold*

undo firewall statistics system connect-number { **frag** | **icmp** | **tcp** | **tcp-proxy** | **udp** }

Parameters

Parameter	Description	Value
frag	Sets the session thresholds of IP fragment packets.	-
icmp	Sets the session thresholds of ICMP packets.	-
tcp	Sets the session thresholds of TCP packets.	-
tcp-proxy	Sets the session thresholds of TCP proxy packets.	-
udp	Sets the session thresholds of UDP packets.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
high *high-threshold*	Specifies the upper threshold of a specified type of protocol packets.	The value is an integer and the value range varies according to product model: • AR120&AR150&AR160&AR200: 1-16384. The default value is 16384. • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 16384. • AR2220, AR2220E: 1-65536. The default value is 65536. • AR2240C: 1-65536. The default value is 65536. • AR2240 and AR3260, SRU40: 1-65536. The default value is 65536. • AR2240 and AR3260, SRU60: 1-160000. The default value is 160000. • AR2204XE, and AR2204XE-DC: 1-204800. The default value is 204800. • AR2240 and AR3260, SRU80 and SRU100E: 1-204800. The default value is 204800. • AR2240 and AR3260, SRU200 and SRU200E: 1-400000. The default value is 400000. • AR2240 and AR3260, SRU400: 1-800000. The default value is 800000. • AR3600 series: 1-400000. The default value is 400000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
low *low-threshold*	Specifies the lower threshold of a specified type of protocol packets.	The value is an integer and the value range varies according to product model: • AR120&AR150&AR160&AR200: 1-16384. The default value is 12288. • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 12288. • AR2220, AR2220E: 1-65536. The default value is 52224. • AR2240C: 1-65536. The default value is 52224. • AR2240, AR3260, and SRU40: 1-65536. The default value is 52224. • AR2240, AR3260, and SRU60: 1-160000. The default value is 52224. • AR2204XE, and AR2204XE-DC: 1-204800. The default value is 163840. • AR2240, AR3260, SRU80 and SRU100E: 1-204800. The default value is 163840. • AR2240, AR3260, SRU200 and SRU200E: 1-400000. The default value is 163840. • AR2240, AR3260,SRU400: 1-800000. The default value is 163840. • AR3600 series: 1-400000. The default value is 163840.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Before setting the session thresholds on the firewall, run the **19.8.57 firewall statistics system enable** command to enable traffic statistics collection on the firewall.

Example

Set the session thresholds of TCP packets on the firewall. Set the upper threshold to 15000 and lower threshold to 10000.

```
<Huawei> system-view
[Huawei] firewall statistics system enable
[Huawei] firewall statistics system connect-number tcp high 15000 low 10000
```

Related Topics

19.8.57 firewall statistics system enable

19.8.14 display firewall statistics system

19.8.57 firewall statistics system enable

Function

The **firewall statistics system enable** command enables traffic statistics collection on the firewall.

The **undo firewall statistics system enable** command disables traffic statistics collection on the firewall.

By default, traffic statistics collection is disabled on the firewall.

Format

firewall statistics system enable

undo firewall statistics system enable

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **19.8.14 display firewall statistics system** command to check whether traffic statistics collection is enabled.

Example

Enable traffic statistics collection on the firewall.

```
<Huawei> system-view
[Huawei] firewall statistics system enable
```

Related Topics

19.8.14 display firewall statistics system

19.8.58 firewall whitelist

Function

The **firewall whitelist** command adds an entry to the whitelist.

The **undo firewall whitelist** command deletes an entry from the whitelist.

Format

firewall whitelist *ip-address* [**vpn-instance** *vpn-instance-name*] [**expire-time** *minutes*]

undo firewall whitelist { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **vpn-instance** *vpn-instance-name* }

Parameters

Parameter	Description	Value
all	Deletes all whitelist entries.	-
ip-address	Specifies the IP address to be added to the whitelist.	The value is a valid IPv4 IP address in dotted decimal notation.
expire-time *minutes*	Specifies the aging time of a whitelist entry.	The value is an integer that ranges from 1 to 1000, in minutes. **NOTE** If this parameter is not set, the entry is always valid.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An IP address cannot exist in both the whitelist and blacklist. To move an IP address from one list to the other list, delete the corresponding entry first.

The entries in the whitelist take effect directly and you do not need to enable the whitelist function.

Example

Add IP address 10.1.1.1 to the whitelist and set the aging time of this entry to 3 minutes.

```
<Huawei> system-view
[Huawei] firewall whitelist 10.1.1.1 expire-time 3
```

Related Topics

19.8.17 display firewall whitelist

19.8.59 firewall zone

Function

The **firewall zone** command creates an interzone.

The **undo firewall zone** command deletes an interzone.

Format

firewall zone *zone-name*

undo firewall zone *zone-name*

Parameters

Parameter	Description	Value
zone-name	Specifies the name of a zone.	The value is a string of 1 to 32 case-sensitive characters without hyphens (-), and must start with a letter.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before configuring a firewall, create zones. Then you can deploy security services according to the security priorities of the zones.

The device considers that the data transmission within a zone is reliable; therefore, it does not enforce any security policy on the intra-zone data transmission.

NOTE

If an interface is added to a zone, the zone cannot be deleted in the system view. To delete the zone, delete the interface from the zone first.

Example

Create the zone **zone1**.

```
<Huawei> system-view
[Huawei] firewall zone zone1
```

Related Topics

19.8.18 display firewall zone

19.8.60 firewall-nat session aging-time

Function

The **firewall-nat session aging-time** command sets the timeout interval of each entry in the session table.

The **undo firewall-nat session aging-time** command restores the default timeout interval of each entry in the session table.

Format

firewall-nat session { { **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time** *time-value*

undo firewall-nat session { { **all** | **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dns	Sets the timeout interval of the DNS protocol.	-
ftp	Sets the timeout interval of the FTP control connection.	-
ftp-data	Sets the timeout interval of the FTP connection.	-
http	Sets the timeout interval of the HTTP connection.	-
icmp	Sets the timeout interval of the ICMP connection.	-
tcp	Sets the timeout interval of the TCP connection.	-
tcp-proxy	Sets the timeout interval of the TCP proxy.	-
udp	Sets the timeout interval of the UDP connection.	-
sip	Sets the timeout interval of the SIP connection.	-
sip-media	Sets the timeout interval of the SIP media protocol.	-
rtsp	Sets the timeout interval of the RTSP protocol.	-
rtsp-media	Sets the timeout interval of the RTSP media protocol.	-
pptp	Sets the timeout interval of the PPTP control connection.	-
pptp-data	Sets the timeout interval of the PPTP connection.	-
all	Restores the default timeout interval of all the preceding connections.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-define *port-number*	Specifies the user-defined TCP or UDP port number and configures the timeout interval for all data connections with this port as the destination port. **NOTE** This parameter only supports NAT and does not support firewall.	The value is an integer that ranges from 1 to 65535.
aging-time *time-value*	Specifies the timeout interval value.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **firewall-nat session aging-time** command sets the timeout interval for sessions of each protocol or port. If an entry in a session table is not used within the specified period, the entry expires. For example, the user with IP address 10.110.10.10 initiates a TCP connection through port 2000. If the TCP connection is not used within the timeout interval, the system deletes the TCP connection.

The default session timeout interval of a port is the same as that of the corresponding protocol. The following table lists the default session timeout interval of each protocol.

Protocol	Default Session Timeout Interval
tcp	600 seconds
tcp-proxy	10 seconds
udp	120 seconds
icmp	20 seconds
dns	120 seconds
http	120 seconds

 Copyright © Huawei Technologies Co., Ltd.

Protocol	Default Session Timeout Interval
ftp	120 seconds
ftp-data	120 seconds
sip	1800 seconds
sip-media	120 seconds
rtsp	60 seconds
rtsp-media	120 seconds
pptp	600 seconds
pptp-data	600 seconds

NOTE

When configuring the timeout interval for all sessions with a user-defined port as the destination port, you cannot set the port number to a default port number of the preceding protocols.

Precautions

For some services such as voice service, increase the TCP/UDP timeout interval to prevent service interruption.

You can set the session timeout interval for a maximum of 24 ports on the device.

Example

Set the timeout interval of the DNS connection to 60 seconds.

```
<Huawei> system-view
[Huawei] firewall-nat session dns aging-time 60
```

Related Topics

19.8.19 display firewall-nat session aging-time

19.8.61 packet-filter

Function

The **packet-filter** command configures packet filtering in an interzone.

The **undo packet-filter** command cancels packet filtering in an interzone.

By default, all outgoing packets are permitted and all incoming packets are denied.

Format

packet-filter { *acl-number* | **default** { **deny** | **permit** } } { **inbound** | **outbound** }

 Copyright © Huawei Technologies Co., Ltd.

undo packet-filter *acl-number* { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
acl-number	Indicates the number of the ACL for packet filtering. The ACLs include basic ACL and advanced ACL.	The value is an integer that ranges from 2000 to 3999: • 2000-2999: basic ACLs • 3000-3999: advanced ACLs
default	Indicates the default packet filtering method.	-
deny	Rejects all packets. **NOTE** This parameter sets the default packet filtering method of the interzone. The default packet filtering method takes effect on all the packets not matching the ACLs.	-
permit	Allows all packets to pass. **NOTE** This parameter sets the default packet filtering method of the interzone. The default packet filtering method takes effect on all the packets not matching the ACLs.	-
inbound	Filters inbound packets. An inbound packet refers to a packet sent from a low-priority zone to a high-priority zone.	-
outbound	Filters outbound packets. An outbound packet refers to a packet sent from a high-priority zone to a low-priority zone.	-

Views

Interzone view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The number of times the command is run cannot exceed the number of configured packet filtering interzones.

Example

Filter the inbound packets in the interzone between zone1 and zone2 by using ACL 3000.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule permit ip
[Huawei-acl-adv-3000] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] packet-filter 3000 inbound
```

Related Topics

19.8.10 display firewall interzone

19.8.62 packet-filter ipv6

Function

The **packet-filter ipv6** command configures IPv6 packet filtering in an interzone.

The **undo packet-filter ipv6** command cancels IPv6 packet filtering in an interzone.

By default, the outbound packets are allowed, and the inbound packets are denied.

Format

packet-filter ipv6 *acl6-number* { **inbound** | **outbound** }

undo packet-filter ipv6 *acl6-number* { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
acl6-number	Indicates the ACL used for packet filtering, including basic ACL6 and advanced ACL6.	The value is an integer that ranges from 2000 to 3999: • 2000-2999: Basic ACL6 • 3000-3999: Advanced ACL6

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
inbound	Filters inbound packets. An inbound packet refers to a packet from a low-priority zone to a high-priority zone.	-
outbound	Filters outbound packets. An outbound packet refers to a packet from a high-priority zone to a low-priority zone.	-

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

The number of times the command is run cannot exceed the number of configured packet filtering interzones.

Example

Filter the inbound IPv6 packets in the interzone between zone1 and zone2 by using ACL6 3000.

```
<Huawei> system-view
[Huawei] acl ipv6 3000
[Huawei-acl6-adv-3000] rule permit ipv6
[Huawei-acl6-adv-3000] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone2-zone1] packet-filter ipv6 3000 inbound
```

Related Topics

19.8.10 display firewall interzone

19.8.63 packet-filter logging

Function

The **packet-filter logging** command enables the packet filtering log in the interzone.

The **undo packet-filter logging** command disables the packet filtering log in the interzone.

By default, the packet filtering log is disabled in the interzone.

 Copyright © Huawei Technologies Co., Ltd.

Format

packet-filter logging [{ **inbound** | **outbound** } [**permit** | **deny**]]

undo packet-filter logging [{ **inbound** | **outbound** } [**permit** | **deny**]]

Parameters

Parameter	Description	Value
inbound	Records logs for incoming packets. An incoming packet refers to a packet from a low-priority zone to a high-priority zone.	-
outbound	Records logs for outgoing packets. An outgoing packet refers to a packet from a high-priority zone to a low-priority zone.	-
permit	Records logs for packets that are allowed to pass through.	-
deny	Records logs for packets that are denied.	-

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the firewall filters packets, a log is recorded if this function is enabled. By analyzing the logs, the network administrator can find potential security threats to the network and take preventive measures to protect the network.

When [{ **inbound** | **outbound** } [**permit** | **deny**]] is not configured, the device records logs for all packets. When { **inbound** | **outbound** } is configured and [**permit** | **deny**] is not configured, the device records logs for incoming or outgoing packets.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

This function takes effect only after the **packet-filter logging** and **firewall log packet-filter enable** commands are executed.

Example

Enable the packet filtering log in the interzone.

```
<Huawei> system-view
[Huawei] firewall zone trust
[Huawei-zone-trust] priority 14
[Huawei-zone-trust] quit
[Huawei] firewall zone untrust
[Huawei-zone-untrust] priority 12
[Huawei-zone-untrust] quit
[Huawei] firewall log packet-filter enable
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] packet-filter logging
```

Related Topics

19.8.53 firewall log enable

19.8.64 port-mapping

Function

The **port-mapping** command configures the mappings between ports and application-layer protocols.

The **undo port-mapping** command deletes the mappings between ports and application-layer protocols.

Format

port-mapping { **dns** | **ftp** | **http** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number*

undo port-mapping { **all** | { **dns** | **ftp** | **http** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number* }

Parameters

Parameter	Description	Value
all	Deletes the mappings from all ports.	-
dns	Specifies the mapping between the DNS protocol and a port.	-
ftp	Specifies the mapping between the FTP protocol and a port.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
http	Specifies the mapping between the HTTP protocol and a port.	-
sip	Specifies the mapping between the SIP protocol and a port.	-
rtsp	Specifies the mapping between the RTSP protocol and a port.	-
pptp	Specifies the mapping between the PPTP protocol and a port.	-
port *port-number*	Specifies the port mapping to a protocol.	The value of *port-number* is an integer that ranges from 1 to 65535.
acl *acl-number*	Specifies the ACL that controls the packets to which port mapping is applied.	The value of *acl-number* is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Port mapping enables a server to provide various application-layer services for external systems through non-well-known ports. For example, the well-known port of the HTTP service is port 80. After port mapping is configured on the firewall, the firewall can use a non-well-known port to provide the HTTP service.

Port mapping reduces attacks to a certain service on the server.

Example

Map the HTTP service to port 10 and apply ACL 2000 to control the packets to which the mapping takes effect.

```
<Huawei> system-view
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule  permit
[Huawei-acl-basic-2000] quit
[Huawei] port-mapping http port 10 acl 2000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.8.20 display port-mapping

19.8.65 priority (security zone view)

Function

The **priority** command sets the priority for a zone.

Format

priority *security-priority*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
security-priority	Indicates the priority of a zone.	The value is an integer and the value range varies according to product models: ● AR100&AR120&AR150&AR160&AR200 series: 0 to 15 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 0 to 15 ● AR2220, AR2220E: 0 to 63 ● AR2240C: 0 to 63 ● AR2240 and AR3260, SRU40 and SRU60: 0 to 63 ● AR2204XE, AR2204XE-DC, AR2240 and AR3260, SRU80 and SRU100E: 0 to 127 ● AR2240 and AR3260, SRU200, SRU200E and SRU400: 0 to 127 ● AR3600 series: 0 to 127 . **NOTE** If *security-priority* is set to a large value, the priority of the zone is high.

Views

Security zone view

Default Level

2: Configuration level

Usage Guidelines

After creating a zone, set a priority for the zone; otherwise, the zone is invalid.

 Copyright © Huawei Technologies Co., Ltd.

The priority of a zone cannot be changed. If you want to change the priority, delete and re-create the zone and reconfigure the priority.

The local zone priority cannot be manually set. The priority of the local zone is the highest priority allowed by the local device plus 1.

Example

Set the priority of zone1 to 5.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] priority 5
```

Related Topics

19.8.18 display firewall zone

19.8.66 reset firewall app table statistics

Function

The **reset firewall app table statistics** command clears statistics on firewall application entries.

Format

reset firewall app { **servermap** | **session** } **table statistics**

Parameters

Parameter	Description	Value
servermap	Clears statistics on Servermap entries at the application layer.	-
session	Clears statistics on session entries at the application layer.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

You can run this command when you need to collect new firewall application entry statistics. After you run this command, all statistics on firewall application entries are cleared.

Precautions

Statistics on firewall application entries cannot be restored after they are cleared. Exercise caution when you use the command.

Example

Clear statistics on firewall session entries at the application layer.

```
<Huawei> system-view
[Huawei] reset firewall app session table statistics
```

Related Topics

19.8.6 display firewall app table statistics

19.8.67 reset firewall ipv6 session all

Function

The **reset firewall ipv6 session all** command deletes all IPv6 entries from the firewall session table.

Format

reset firewall ipv6 session all

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command can delete all entries in a firewall session table.

Precautions

This command deletes entries from the firewall session table and modifies the firewall configurations immediately.

After this command is executed, you must wait at least 10 seconds if you need to run the command again; otherwise, a warning message is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete all IPv6 entries from a firewall session table.

```
<Huawei> system-view
[Huawei] reset firewall ipv6 session all
Warning:The current all firewall ipv6 sessions will be deleted.
Are you sure to continue?[Y/N]y
```

19.8.68 reset firewall session

Function

The **reset firewall session** command deletes entries from the firewall session table.

Format

reset firewall session all

reset firewall session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]]

reset firewall session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]]

reset firewall session destination *destination-address* [*destination-port*]

NOTE

V200R010C10 and later versions support the **protocol**, **source**, and **destination** parameters.

Parameters

Parameter	Description	Value
all	Deletes all entries from the firewall session table.	-
protocol { *protocol-number* | *protocol-name* }	Deletes entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMP, TCP, or UDP.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source *source-address* [*source-port*]	Deletes entries with a specified source IP address or both a source IP address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• *source-address* is in dotted decimal notation. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Deletes entries with a specified destination IP address or both a destination IP address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• *destination-address* is in dotted decimal notation. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command will delete entries from a firewall session table.

Precautions

After this command is executed, entries are deleted from the firewall session table and the firewall configurations are modified immediately.

After this command is executed, you must wait at least 10 seconds before running the command again; otherwise, an error message is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete all entries from a firewall session table.

```
<Huawei> system-view
[Huawei] reset firewall session all
Warning:The current all firewall sessions will be deleted.
Are you sure to continue?[Y/N]y
```

19.8.69 reset session

Function

The **reset session** command deletes entries from the session table.

Format

reset session all

reset session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]]

reset session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]]

reset session destination *destination-address* [*destination-port*]

NOTE

V200R010C10 and later versions support the **protocol**, **source**, and **destination** parameters.

Parameters

Parameter	Description	Value
all	Deletes all entries from the session table.	-
protocol { *protocol-number* | *protocol-name* }	Deletes entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMP, TCP, or UDP.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source *source-address* [*source-port*]	Deletes entries with a specified source IP address or both a source IP address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• *source-address* is in dotted decimal notation. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Deletes entries with a specified destination IP address or both a destination IP address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• *destination-address* is in dotted decimal notation. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command will delete entries from a firewall or NAT session table.

Precautions

After this command is executed, entries are deleted from session tables and the session table configurations are modified immediately.

After this command is executed, you must wait at least 10 seconds before running the command again; otherwise, an error message is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete all entries from a session table.

```
<Huawei> system-view
[Huawei] reset session all
Warning:The current all sessions will be deleted.
Are you sure to continue?[Y/N]y
```

19.8.70 reset firewall statistics system defend

Function

The **reset firewall statistics system defend** command deletes attack defense statistics on firewall.

Format

reset firewall statistics system defend

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

Before you run the **display firewall statistics system defend** command to collect attack defense statistics on a firewall, you can run this command to delete the old statistics.

Precautions

Statistics cannot be restored after they are cleared. Exercise caution when you delete them.

Example

Delete attack defense statistics on the firewall.

```
<Huawei> reset firewall statistics system defend
```

Related Topics

19.8.14 display firewall statistics system

 Copyright © Huawei Technologies Co., Ltd.

19.8.71 session-log

Function

The **session-log** command configures a condition for recording logs about sessions in the firewall interzone.

The **undo session-log** command deletes a condition for recording logs about sessions in the firewall interzone.

By default, no condition is configured for recording logs about sessions in the firewall interzone.

Format

session-log *acl-number* { **inbound** | **outbound** }

undo session-log *acl-number* { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL used to match sessions.	The value is an integer that ranges from 2000 to 3999.
inbound	Applies the ACL to the inbound sessions. **NOTE** An inbound session refers to a session from a low-priority zone to a high-priority zone.	-
outbound	Applies the ACL to the outbound sessions. **NOTE** An outbound session refers to a high-priority session sent from a zone to a low-priority zone.	-

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Create zone1 and zone2, and set their priorities to 10 and 5 respectively. Then configure an interzone between zone1 and zone2, and record logs about the inbound sessions (from zone 1 to zone 2) that match ACL 2001.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] priority 10
[Huawei-zone-zone1] quit
[Huawei] firewall zone zone2
[Huawei-zone-zone2] priority 5
[Huawei-zone-zone2] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] session-log 2001 inbound
[Huawei-interzone-zone1-zone2] quit
[Huawei] firewall log session enable
```

Related Topics

19.8.53 firewall log enable

19.8.10 display firewall interzone

19.8.72 statistics connect-number ip

Function

The **statistics connect-number ip** command sets the thresholds for the number of sessions on an IP address.

The **undo statistics connect-number ip** command restores the default thresholds.

Format

statistics connect-number ip [**range** *beginip endip*] { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** } **high** *high-threshold* **low** *low-threshold*

undo statistics connect-number ip { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** }

Parameters

Parameter	Description	Value
range	Specified an IP address segment **NOTE** If the **range** parameter is not specified, this command takes effect on a single IP address.	-
beginip	Specifies the start IP address.	The value is in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
endip	Specified the end IP address, which cannot be smaller than the start IP address. The start and end IP addresses must be in the same IP address segment.	The value is in dotted decimal notation.
inzone	Specifies the thresholds for the number of packets entering the zone.	-
outzone	Specifies the thresholds for the number of packets leaving the zone.	-
icmp	Specifies the thresholds for the number of ICMP packets.	-
tcp	Specifies the thresholds for the number of TCP packets.	-
udp	Specifies the thresholds for the number of UDP packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
high *high-threshold*	Specifies the upper threshold value.	The value is an integer and the value range depends on the product type: ● AR120&AR150&AR160&AR200: 1-16384. The default value is 16384. ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 16384. ● AR2220, AR2220E: 1-65536. The default value is 65536. ● AR2240C: 1-65536. The default value is 65536. ● AR2240 and AR3260, SRU40: 1-65536. The default value is 65536. ● AR2240 and AR3260, SRU60: 1-160000. The default value is 160000. ● AR2204XE, and AR2204XE-DC: 1-204800. The default value is 204800. ● AR2240 and AR3260, SRU80 and SRU100E: 1-204800. The default value is 204800. ● AR2240 and AR3260, SRU200 and SRU200E: 1-400000. The default value is 400000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• AR2240 and AR3260, SRU400: 1-800000. The default value is 800000. • AR3600 series: 1-400000. The default value is 400000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
low *low-threshold*	Sets the lower thresholds value.	The value is an integer and the value range depends on the product type: • AR120&AR150&AR160&AR200: 1-16384. The default value is 12288. • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 12288. • AR2220, AR2220E: 1-65536. The default value is 52224. • AR2240C: 1-65536. The default value is 52224. • AR2240, AR3260, and SRU40: 1-65536. The default value is 52224. • AR2240, AR3260, and SRU60: 1-160000. The default value is 52224. • AR2204XE, and AR2204XE-DC: 1-204800. The default value is 163840. • AR2240, AR3260, SRU80 and SRU100E: 1-204800. The default value is 163840. • AR2240, AR3260, SRU200 and SRU200E: 1-400000. The default value is 163840.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• AR2240, AR3260,SRU400: 1-800000. The default value is 163840. • AR3600 series: 1-400000. The default value is 163840.

Views

Security zone view

Default Level

2: Configuration level

Usage Guidelines

Before setting the thresholds for the number of packets sent to a certain IP address, run the **19.8.74 statistics ip enable** command to enable the IP address-level traffic statistics function in the zone.

Example

Configure the thresholds for the number of inbound TCP packets sent to a certain IP address. Set the upper threshold to 15000 and lower threshold to 10000.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] statistics ip enable inzone
[Huawei-zone-zone1] statistics connect-number ip inzone tcp high 15000 low 10000
```

Related Topics

19.8.74 statistics ip enable

19.8.16 display firewall statistics zone-ip

19.8.73 statistics connect-number zone

Function

The **statistics connect-number zone** command sets the thresholds for the number of packets in a zone.

The **undo statistics connect-number zone** command restores the default thresholds for the number of packets in a zone.

 Copyright © Huawei Technologies Co., Ltd.

Format

statistics connect-number zone { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** } **high** *high-threshold* **low** *low-threshold*

undo statistics connect-number zone { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** }

Parameters

Parameter	Description	Value
inzone	Specifies the thresholds for the number of packets entering the zone.	-
outzone	Specifies the thresholds for the number of packets leaving the zone.	-
icmp	Specifies the thresholds for the number of ICMP packets.	-
tcp	Specifies the thresholds for the number of TCP packets.	-
udp	Specifies the thresholds for the number of UDP packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
high *high-threshold*	Specifies the upper threshold value.	The value is an integer and the value range varies according to product models: • AR120&AR150&AR160&AR200: 1-16384. The default value is 16384. • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 16384. • AR2220, AR2220E: 1-65536. The default value is 65536. • AR2240C: 1-65536. The default value is 65536. • AR2240 and AR3260, SRU40: 1-65536. The default value is 65536. • AR2240 and AR3260, SRU60: 1-160000. The default value is 160000. • AR2204XE, and AR2204XE-DC: 1-204800. The default value is 204800. • AR2240 and AR3260, SRU80 and SRU100E: 1-204800. The default value is 204800. • AR2240 and AR3260, SRU200 and SRU200E: 1-400000. The default value is 400000. • AR2240 and AR3260, SRU400: 1-800000. The default value is 800000. • AR3600 series: 1-400000. The default value is 400000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
low *low-threshold*	Specifies the lower threshold value.	The value is an integer and the value range varies according to product models: • AR120&AR150&AR160&AR200: 1-16384. The default value is 12288. • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 12288. • AR2220, AR2220E: 1-65536. The default value is 52224. • AR2240C: 1-65536. The default value is 52224. • AR2240, AR3260, and SRU40: 1-65536. The default value is 52224. • AR2240, AR3260, and SRU60: 1-160000. The default value is 52224. • AR2204XE, and AR2204XE-DC: 1-204800. The default value is 163840. • AR2240, AR3260, SRU80 and SRU100E: 1-204800. The default value is 163840. • AR2240, AR3260, SRU200 and SRU200E: 1-400000. The default value is 163840. • AR2240, AR3260,SRU400: 1-800000. The default value is 163840. • AR3600 series: 1-400000. The default value is 163840.

Views

Security zone view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Before setting the thresholds for the number of packets in a zone, run the **19.8.75 statistics zone enable** command to enable the zone-level traffic statistics function.

Example

Configure the thresholds for the number of inbound TCP packets in a zone. Set the upper threshold to 15000 and lower threshold to 10000.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] statistics zone enable inzone
[Huawei-zone-zone1] statistics connect-number zone inzone tcp high 15000 low 10000
```

Related Topics

19.8.75 statistics zone enable

19.8.15 display firewall statistics zone

19.8.74 statistics ip enable

Function

The **statistics ip enable** command enables the IP address-level traffic statistics collection in a zone.

The **undo statistics ip enable** command disables the IP address-level traffic statistics collection in a zone.

By default, IP address-level traffic statistics collection is disabled.

Format

statistics ip enable { **inzone** | **outzone** }

undo statistics ip enable { **inzone** | **outzone** }

Parameters

Parameter	Description	Value
inzone	Enables the IP address-level traffic statistics collection for the inbound packets of the zone.	-
outzone	Enables the IP address-level traffic statistics collection for the outbound packets of the zone.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Security zone view

Default Level

2: Configuration level

Usage Guidelines

The IP address-based traffic statistics collection counts and monitors the TCP and UDP sessions set up by an IP address in a zone. When the number of TCP and UDP sessions set up by the IP address exceeds the threshold, the device reduces the number of sessions to the specified range.

You can enable IP address-level traffic statistics collection for inbound or outbound packets of a zone.

Inbound packets are sent from other zones to the local zone. Outbound packets are sent from the local zone to other zones.

NOTE

When both IP traffic statistics collection and fast ICMP reply are enabled on an AR160 or AR200, outbound IP traffic statistics are not collected.

Example

Enable IP address-level traffic statistics collection for inbound packets and outbound packets in zone1.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] statistics ip enable inzone
[Huawei-zone-zone1] statistics ip enable outzone
```

Related Topics

19.8.72 statistics connect-number ip

19.8.16 display firewall statistics zone-ip

19.8.75 statistics zone enable

Function

The **statistics zone enable** command enables zone-level traffic statistics collection for the packets in a zone.

The **undo statistics zone enable** command disables zone-level traffic statistics collection for the packets in a zone.

By default, zone-level traffic statistics collection is disabled.

Format

statistics zone enable { **inzone** | **outzone** }

 Copyright © Huawei Technologies Co., Ltd.

undo statistics zone enable { **inzone** | **outzone** }

Parameters

Parameter	Description	Value
inzone	Enables zone-level traffic statistics collection for the inbound packets of the zone.	-
outzone	Enables zone-level traffic statistics collection for the outbound packets of the zone.	-

Views

Security zone view

Default Level

2: Configuration level

Usage Guidelines

You can enable zone-level traffic statistics collection for inbound or outbound packets in a zone.

Example

Enable zone-level traffic statistics collection for inbound packets and outbound packets of zone1.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] statistics zone enable inzone
[Huawei-zone-zone1] statistics zone enable outzone
```

Related Topics

19.8.15 display firewall statistics zone

19.8.76 zone

Function

The **zone** command adds an interface to a zone.

The **undo zone** command deletes an interface from a zone.

Format

zone *zone-name*

 Copyright © Huawei Technologies Co., Ltd.

undo zone

Parameters

Parameter	Description	Value
zone-name	Specifies the name of a zone.	The value is a string of 1 to 32 characters without hyphens (-), and must start with a letter.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When you add an interface to a zone, ensure that the zone has been created using the **19.8.59 firewall zone** command.

NOTE

This command can only be used on Layer 3 interfaces, except the Loopback, NULL, Bridge-if, and Tunnel-Template interfaces.

Example

Add GE1/0/0 to zone1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] zone zone1
```

Related Topics

19.8.59 firewall zone

19.8.18 display firewall zone

19.9 Deep Security Configuration Commands

19.9.1 Security Policy Configuration Commands

NOTE

AR161, AR161F, AR161F-DGP, AR161FG-L, AR161FGW-L, AR161FGW-La, AR161FGW-Lc, AR161FW-P-M5, AR161G-L, AR161G-Lc, AR161G-U, AR161W, AR162F, AR168F, AR169, AR169-P-M9, AR169CVW, AR169CVW-4B4S, AR169F, AR169G-L, AR169W-P-M9, AR169RW-P-M9, and AR3670 do not support the security policy.

 Copyright © Huawei Technologies Co., Ltd.

19.9.1.1 display engine information

Function

The **display engine information** command displays the status of IAE (Intelligent Awareness Engine) and the version of all signature databases.

Format

display engine information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the status of IAE and the version of all signature databases.

```
<Huawei> display engine information
================================================================================

Engine on CPU 0 in slot 0:
================================================================================

  Engine Status                  : Ready
  Compile Status                 : Idle
  IPS Engine Version             : V200R003C00SPC008
  IPS Signature Database Version   : 2017011104
  SA Signature Database Version    : 2017041201
  C&C Domain Name Database Version :
--------------------------------------------------------------------------------
```

Table 19-97 Description of the **display engine information** command output

Item	Description
Engine on CPU *X* in slot *Y*	Engine information on CPU *X* in slot *Y*
Engine Status	Engine status, which can be: ● Not Run: The engine is not running. ● Initializing: The engine is initializing. ● Ready: The engine is ready.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Compile Status	Compilation status, which can be: • Idle: The engine status is idle. • Committing: The configuration is being committed. • Commit Succeeded: Succeeded in committing the configuration. • Commit Failed: Failed to commit the configuration. • Commit Time Out: Committing the configuration timed out. • Updating: The signature database is being updated. • Update Succeeded: Succeeded in updating the signature database. • Update Failed: Failed to update the signature database. • Update Time Out: Updating the signature database timed out.
IPS Engine Version	Version of the IPS engine
IPS Signature Database Version	Version of the IPS signature database
SA Signature Database Version	Version of the application identification signature database used by the Router
C&C Domain Name Database Version	Version of the malicious domain name signature database

19.9.1.2 display security-policy

Function

The **display security-policy** command displays the security policy configuration.

Format

display security-policy { **all** | **name** *policy-name* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
all	Displays the configuration of all security policies.	-
name *policy-name*	Displays the configuration of a specified security policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the configuration of a specified security policy or all security policies.

Example

Display the configuration of all security policies.

```
<Huawei> display security-policy all
  Policy-name: huawei
  Policy-ID: 0
   IPS: -
   URLF: -
   ACL: 0
  Reference-Num: 0
```

Display the configuration of the security policy **huawei**.

```
<Huawei> display security-policy name huawei
  Policy-name: huawei
  Policy-ID: 0
   IPS: -
   URLF: -
   ACL: 0
  Reference-Num: 0
```

Table 19-98 Description of the display security-policy command output

Item	Description
Policy-name	Name of the security policy. To configure a security policy, run the **19.9.1.15 security-policy** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Policy-ID	ID of the security policy.
IPS	IPS profile bound to the security policy. To bind an IPS profile to a security policy, run the **19.9.1.14 profile (security policy view)** command.
URLF	URL filtering profile bound to the security policy. To bind a URL filtering profile to a security policy, run the **19.9.1.14 profile (security policy view)** command.
ACL	ACL bound to the security policy. To bind an ACL to a security policy, run the **19.9.1.14 profile (security policy view)** command.
Reference-Num	Total number of profiles in the security policy.

Related Topics

19.9.1.15 security-policy
19.9.1.14 profile (security policy view)

19.9.1.3 display update configuration

Function

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

Format

display update configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Display the update configuration.

```
<Huawei> display update configuration
Update Configuration Information:
-------------------------------------------------------------
  Update Server              : sec.huawei.com
  Update Port                : 443
  Proxy State                : Disable
  Proxy Server               : -
  Proxy Port                 : -
  Proxy User                 : -
  Proxy Password             : -
  IPS-SDB:
    Application Confirmation  : Disable
    Schedule Update           : Enable
    Schedule Update Frequency : Daily
    Schedule Update Time      : 03:35
  SA-SDB:
    Application Confirmation  : Disable
    Schedule Update           : Enable
    Schedule Update Frequency : Daily
    Schedule Update Time      : 03:35
  CNC:
    Application Confirmation  : Disable
    Schedule Update           : Enable
    Schedule Update Frequency : Daily
    Schedule Update Time      : 03:35
-------------------------------------------------------------
```

Table 19-99 Description of the **display update configuration** command output

Item	Description
Update Server	IP address or domain name of the update server. The default domain name is sec.huawei.com.
Update Port	Port number of the update server.
Proxy State	Whether the proxy server is enabled. The value can be: ● Enable: The proxy server is enabled. ● Disable: The proxy server is disable.
Proxy Server	IP address or domain name of the proxy server.
Proxy Port	Port number of the proxy server.
Proxy User	User name of the proxy server.
Proxy Password	Password of the proxy server.
IPS-SDB	Update configuration of the IPS-SDB.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Application Confirmation	Whether manual installation confirmation is enabled. The value can be: • Enable: Confirmation is required before the installation of the update file. • Disable: The update file is automatically installed.
Schedule Update	Whether the scheduled update function is enabled. The value can be: • Enable • Disable
Schedule Update Frequency	Scheduled update frequency. The value can be: • Weekly • Daily • Hourly
Schedule Update Time	Scheduled update time
SA-SDB	Update configuration of the application signature database
CNC	Update configuration of the malicious domain name database

19.9.1.4 display update information all-sdb

Function

The **display update information all-sdb** command displays the last record on signature database updates.

Format

display update information all-sdb

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To display the last record on signature database updates, run the **display update information all-sdb** command.

Example

Display the last record on signature database updates.

```
<Huawei> display update information all-sdb

Current Update Status:  Idle.
-------------------------------------------------------------------------------
 IPS-SDB latest update finish time      : 05:17:05 2017/01/24
 IPS-SDB latest update result           : Info: The IPS-SDB update succeeded.
-------------------------------------------------------------------------------
 SA-SDB latest update finish time       : 05:17:24 2017/01/24
 SA-SDB latest update result            : Info: The SA-SDB update succeeded.
-------------------------------------------------------------------------------
 CNC latest update finish time          : 05:17:37 2017/01/24
 CNC latest update result               : Info: No version for loading CNC.
-------------------------------------------------------------------------------
```

Table 19-100 Description of the **display update information all-sdb** command output

Item	Description
Current Update Status	Status of the update server: • Idle: indicates that no signature database is being updated. • Version Loading: indicates that the version is being loaded. • Live Updating: indicates live update. • Local Updating: indicates the local update. • Version Rollbacking: indicates that version rollback is being performed. • Stop Updating: indicates that the update is being stopped. • Version Applying: indicates that the version is being downloaded. • Version Restoring: indicates that the default version is being restored. • Version Uninstalling: indicates that the version is being uninstalled. • Update check: indicates that the update is being checked. • Engine start loading: indicates that the engine start is being loaded.
latest update finish time	Last update time of the signature database

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
latest update result	Last update result of the signature database
IPS-SDB	IPS signature database
SA-SDB	Service awareness signature database
CNC	Malicious domain name database

19.9.1.5 display update host source

Function

The **display update host source** command displays the interface and source address configurations used in online update.

Format

display update host source

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays the configurations of the **update host source** command.

Example

Display the interface and source address configurations used in online update.

```
<Huawei> display update host source
-------------------------------------------------------------------
Source IP Information:
      IP address              : 10.1.1.1
Source Interface Information:
      interface name          : GigabitEthernet1/0/0
-------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-101 Description of the **display update host source** command output

Item	Description
Source IP Information	Source IP address information
IP address	IP address
Source Interface Information	Source interface information
interface name	Interface name

19.9.1.6 display update status

Function

The **display update status** command displays the update status.

Format

display update status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

View the current update status.

```
<Huawei> display update status
  Current Update Status: Idle.
```

The update status of a database. The update status includes the update type and update status. The details are as follows:

Update type:

- Idle: indicates that no signature database is being updated.

 Copyright © Huawei Technologies Co., Ltd.

- Version Load: indicates that the version is being loaded.
- Online Update: indicates online update.
- Local Update: indicates the local update.
- Version Rollback: indicates the version rollback.
- Stop Update: indicates that the update is stopped.
- Version Apply: indicates that the version is applied.
- Version Restore: indicates that the default version is restored.
- Version Uninstall: indicates that the version is being uninstalled.
- Update check: indicates that the update is checked.
- Engine start loading: indicates that the engine start is being loaded.

Update status:

- Ready to load The Update Package: indicates that the update package will be loaded soon.
- Verify The Authority: indicates that permission is being verified.
- Obtain The Update Package: indicates that the update package is being obtained.
- Load The Update Package: indicates that the update package is being loaded.
- Merge The Incremental Package: indicates that the incremental package is being merged.
- Retry The Update: indicates that the update is being retried.

For example:

- Online Update, Obtain The Update Package.: indicates online update and an update package is being downloaded.
- Version Rollback, Load The Update Package: indicates version rollback and a rollback package is being loaded.
- Version Apply, Verify The Authority.: indicates that the version is being applied and the permission is being verified.
- Local Update, Load The Update Package.: indicates local update and a update package is being loaded.

19.9.1.7 display version (security policy)

Function

The **display version** command displays version information of the IAE and signature database.

Format

display version { **engine** | **ips-sdb** | **sa-sdb** } *

Parameters

Parameter	Description	Value
engine	Displays version information of the intelligent awareness engine.	-
ips-sdb	Displays version information of the IPS signature database.	-
sa-sdb	Displays version information of the service awareness (SA) signature database.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display version information of the IPS signature database.

```
<Huawei> display version ips-sdb
IPS SDB Update Information List:
------------------------------------------------------------------
 Current Version  :
   Signature Database Version    : 2012090600
   Signature Database Size(byte) : 28032
   Update Time                   : 08:34:03 2012/09/06
   Issue Time of the Update File : 00:00:33 2012/09/06

 Backup Version   :
   Signature Database Version    : 2012090600
   Signature Database Size(byte) : 26752
   Update Time                   : 07:18:56 2002/09/06
   Issue Time of the Update File : 20:11:40 2009/09/06

 Download Version:
   Signature Database Version    :
   Signature Database Size(byte) : 0
------------------------------------------------------------------
```

Table 19-102 Description of the **display version** command output

Item	Description
Current Version	The following parameters indicate information about the current signature database.
Signature Database Version	Signature database version.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Signature Database size	Signature database size.
Update Time	The update time of the signature database, that is, the installation time of the update package.
Issue Time of the Update File	Release time of the update file. You can use the time to determine whether the update package is the latest.
Backup Version	The following parameters indicate information about. The signature database is rolled back to the version if you run the **update rollback** command.
Download Version	The following parameters indicate version information about the newly downloaded the intelligent awareness engine or signature database. The version installation is waiting for your confirmation. If the signature database size and time are 0, no version is downloaded. If you run the **undo update confirm** command to disable the automatic installation confirmation function, this information is not displayed.

19.9.1.8 engine configuration commit

Function

The **engine configuration commit** command commits the configuration of security policies.

Format

engine configuration commit

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Newly configured security policies or the modified security policies do not take effect until you run the **engine configuration commit** command to commit the

 Copyright © Huawei Technologies Co., Ltd.

configuration. To save time, commit the configurations in batches after you have completed all security policy configurations.

Before committing configurations, ensure that the IAE is available. Otherwise the configurations committed using the **engine configuration commit** command do not take effect.

Example

Commit the security policy configurations.

```
<Huawei> system-view
[Huawei] engine configuration commit
```

19.9.1.9 engine enable

Function

The **engine enable** command enables the deep security function.

The **undo engine enable** command disables the deep security function.

By default, the system disables the deep security function.

Format

engine enable

undo engine enable

Parameters

none

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use the IPS or URL filtering function, you need to purchase a license and run the **engine enable** command to enable the deep security function.

Precautions

To disable deep security, run the **undo engine enable** command, and restart the device. After the device restarts, the deep security configurations are deleted.

Example

Enable the deep security function.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] engine enable
```

Related Topics

19.9.1.1 display engine information

19.9.1.10 engine enhanced-detection

Function

The **engine enhanced-detection** command configures the engine to work in enhanced detection mode.

The **undo engine enhanced-detection** command configures the engine to work in common detection mode.

Format

engine enhanced-detection

undo engine enhanced-detection

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the engine works in common detection mode.

After you configure the engine to work in enhanced detection mode, the detection capability of the device will be enhanced, and the detection speed will be decreased.

Example

Configure the engine to work in enhanced detection mode.

```
<Huawei> system-view
[Huawei] engine enhanced-detection
```

19.9.1.11 engine log enable

 Copyright © Huawei Technologies Co., Ltd.

Function

The **engine log enable** command enables the log generation function for a specific module.

The **undo engine log enable** command disables the log generation function for a specified module.

Format

engine log { **ips** | **url-filter** } **enable**

undo engine log { **ips** | **url-filter** } **enable**

Parameters

Parameter	Description	Value
ips	Indicates intrusion prevention.	-
url-filter	Indicates URL filtering.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the log generation function is enabled for all modules.

Example

Enable the log generation function for IPS module.

```
<Huawei> system-view
[Huawei] engine log ips enable
```

19.9.1.12 engine log timeout

Function

The **engine log timeout** command sets the period for caching IPS and URL filtering logs.

The **undo engine log timeout** command restores the default period for caching IPS and URL filtering logs.

By default, the period for caching IPS and URL filtering logs is 1 minute.

 Copyright © Huawei Technologies Co., Ltd.

Format

engine log timeout *interval*

undo engine log timeout

Parameters

Parameter	Description	Value
interval	Specifies the period for caching IPS and URL filtering logs.	The value is an integer that ranges from 0 to 30, in minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the period for caching logs to control the frequency for sending IPS and URL filtering logs.

For example, if many intrusions occur on the IPS-enabled device in a given period of time, the IPS module reports many logs to the device in a short time. If the device outputs logs in real time, the administrator has to flood the screen. After the period for caching logs is set, the device outputs logs only when the period is reached. This prevents the impact of log output.

Precautions

The log buffer records a maximum of 1024 logs, and outputs 16 logs each time. The output logs are deleted from the buffer.

Example

Set the period for caching IPS and URL filtering logs to 5 minutes.

```
<Huawei> system-view
[Huawei] engine log timeout 5
```

19.9.1.13 engine pass-through enable

Function

The **engine pass-through enable** command enables the pass-through mode of the engine.

 Copyright © Huawei Technologies Co., Ltd.

The **undo engine pass-through enable** command disables the pass-through mode of the engine.

Format

engine pass-through enable

undo engine pass-through enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

The pass-through mode of the engine is disabled by default.

After the pass-through mode of the engine is enabled, the system generates events, such as debugging information or log during service processing, but does not perform actual actions. Even a block action is configured for a service, the system does not block traffic but records the service event state.

Example

Enable the pass-through mode of the engine.

```
<Huawei> system-view
[Huawei] engine pass-through enable
```

19.9.1.14 profile (security policy view)

Function

The **profile** command binds an IPS or URL filtering profile to a security policy.

The **undo profile** command unbinds an IPS or URL filtering profile from a security policy.

By default, no IPS or URL filtering profile is bound to a security policy.

Format

profile { **ips** *ips-name* | **urlf** *urlf-name* } * [**acl** *acl-id*]

undo profile

Parameters

Parameter	Description	Value
ips *ips-name*	Specifies the name of an IPS profile bound to a security policy.	The value is a string of case-sensitive characters. The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-). • If the value of *ips-name* does not contain any space, the value contains 1 to 32 characters. • If the value of *ips-name* contains spaces, you must enclose the value with double quotation marks (""), for example, "user for test", and the value contains 3 to 34 characters.
urlf *urlf-name*	Specifies the name of a URL filtering profile bound to a security policy.	The value is a string of case-sensitive characters. The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-). • If the value of *urlf-name* does not contain any space, the value contains 1 to 32 characters. • If the value of *urlf-name* contains spaces, you must enclose the value with double quotation marks (""), for example, "user for test", and the value contains 3 to 34 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl *acl-id*	Specifies the number of an ACL. If no ACL is specified, the device detects all traffic passing through interzones.	The value is an integer. • 2000 to 2999: basic ACLs • 3000 to 3999: advanced ACLs

Views

Security policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses a security policy to implement integrated detection of content security.

Integrated detection of content security indicates that the device uses the Intelligent Awareness Engine to detect and process the content of one flow at one time, implementing content security functions including intrusion defense IPS or URL filtering.

After this command binds an IPS or URL filtering profile to a security policy and the security policy is applied to an interzone, the device performs IPS or URL filtering for traffic passing through the interzone.

Prerequisites

- A URL filtering profile has been created using the **19.9.3.19 profile type url-filter name** command if the URL filtering profile needs to be bound to a security policy.
- An IPS profile has been created using the **profile type ips name** command if the IPS profile needs to be bound to a security policy.
- An ACL has been created using the **19.7.4 acl (system view)** command if the ACL needs to be bound to a security policy.

Precautions

To configure various content security protection functions (for example, URL filtering and IPS need to be configured simultaneously), configure a URL filtering profile and IPS profile, and run the **profile** command to bind the URL filtering profile and IPS profile to a security policy.

If a security policy has been applied to the interzone using the **19.9.1.16 security-policy (interzone view)** command, run the **undo security-policy** command to unbind the security policy from the interzone, and then bind the IPS or URL filtering profile to the security policy.

 Copyright © Huawei Technologies Co., Ltd.

Currently, only ACL4 is supported for IPS or URL filtering. When an ACL is bound to a security policy, pay attention to the following points:

- If the ACL rule defines a permit clause, the device detects traffic matching the ACL rule.
- If the ACL rule defines a deny clause, the device does not detect traffic matching the ACL rule.
- If traffic does not match the ACL, the device does not detect the traffic.

Example

Bind a URL filtering profile **huawei** to a security policy **huawei**.

```
<Huawei> system-view
[Huawei] profile type url-filter name huawei
[Huawei-profile-url-filter-huawei] quit
[Huawei] security-policy huawei
[Huawei-security-policy-huawei] profile urlf huawei
```

Bind a IPS profile **huawei** to a security policy **huawei**.

```
<Huawei> system-view
[Huawei] profile type ips name huawei
[Huawei-profile-ips-huawei] quit
[Huawei] security-policy huawei
[Huawei-security-policy-huawei] profile ips huawei
```

Related Topics

19.9.1.16 security-policy (interzone view)

19.9.2.53 profile type ips name

19.9.3.19 profile type url-filter name

19.9.1.15 security-policy

Function

The **security-policy** command creates a security policy and displays its view, or directly displays the view of an existing security policy.

The **undo security-policy** command deletes a security policy.

By default, no security policy is created.

Format

security-policy *policy-name*

undo security-policy *policy-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a security policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As the network develops continuously, there are various types of potential risks such as Trojan horses, worms, and viruses in packets. Packet filtering rules based on the 5-tuple (source address, destination address, source port, destination port, protocol type) used to control traffic forwarding cannot meet requirements. Enterprises require more secure methods to protect network security.

To monitor network traffic, the device uses a security policy to implement integrated detection of content security. Integrated detection of content security indicates that the device uses the Intelligent Awareness Engine to detect and process the content of one flow at one time, implementing content security functions including intrusion defense and URL filtering. By configuring a security policy, the device controls traffic forwarding based on users and applications, provides traffic content security detection, and implements content security functions of intrusion defense, and URL filtering to ensure network security.

Follow-up Procedure

Run the **19.9.1.16 security-policy (interzone view)** command to create an interzone and enter the interzone view.

Example

Create a security policy **security**.

```
<Huawei> system-view
[Huawei] security-policy security
[Huawei-security-policy-security]
```

Related Topics

19.9.1.16 security-policy (interzone view)

19.9.1.2 display security-policy

 Copyright © Huawei Technologies Co., Ltd.

19.9.1.16 security-policy (interzone view)

Function

The **security-policy** command binds a security policy to an interzone.

The **undo security-policy** command unbinds a security policy from an interzone.

By default, no security policy is bound to an interzone.

Format

security-policy *policy-name*

undo security-policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a security policy to be bound to an interzone.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A security policy must be bound to an interzone so that IPS or URL filtering in the security policy can be used to defend against application layer attacks (for example, buffer overflow attacks, Trojan horses, and worms attacks) or control HTTP access rights.

Prerequisites

The **19.8.51 firewall interzone** command has been executed to create an interzone and enter the interzone view.

The **19.9.1.15 security-policy** command has been executed to create a security policy.

Example

Bind the security policy **security** to an interzone.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] priority 10
[Huawei-zone-zone1] quit
[Huawei] firewall zone zone2
[Huawei-zone-zone2] priority 13
[Huawei-zone-zone2] quit
[Huawei] security-policy security
[Huawei-security-policy-security] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] security-policy security
```

Related Topics

19.8.10 display firewall interzone

19.9.1.17 update abort

Function

The **update abort** command aborts the update process.

Format

update abort

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

The **update abort** command can only be used for online/immediate updates or update retries. In online/immediate updates, the device needs to connect to the update center. If the network rate is too low and impacts the services and device performance, you can run the **update abort** command to abort the update and then retry updating when appropriate. In update retires, you cannot perform other update operations. If you need to use another update method, run the **update abort** command to abort the update process first.

Example

Abort the update process.

```
<Huawei> system-view
[Huawei] update online cnc
[Huawei] update abort
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.1.18 update apply

Function

The **update apply** command installs the downloaded update files.

Format

update apply { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Installs the malicious domain name database update files.	-
ips-sdb	Installs the IPS signature database update files.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

If manual installation confirmation has been enabled by the **update confirm** command, run the **update apply** command to install the update files. If update files have been uploaded to the device memory using FTP, run the **update local** command to install them.

Example

Install the malicious domain name database update files.

```
<Huawei> system-view
[Huawei] update apply cnc
```

19.9.1.19 update confirm

Function

The **update confirm** command enables manual confirmation of database installation.

The **undo update confirm** command disables manual confirmation of database installation.

 Copyright © Huawei Technologies Co., Ltd.

Format

update confirm { **cnc** | **ips-sdb** | **sa-sdb** } **enable**

undo update confirm { **cnc** | **ips-sdb** | **sa-sdb** } **enable**

Parameters

Parameter	Description	Value
cnc	Indicates the malicious domain name database.	-
ips-sdb	Indicates the IPS signature database.	-
sa-sdb	Indicates the application identification signature database.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The manual confirmation of database installation is disabled by default. That is, the device automatically installs the upgrade files after downloading them.

If you enable manual confirmation of database installation, the device will not automatically install the upgrade files after downloading them. You need to run the **update apply** command to install the upgrade files.

Example

Disable manual confirmation for the malicious domain name database installation.

```
<Huawei> system-view
[Huawei] undo update confirm cnc enable
```

19.9.1.20 update force apply

Function

The **update force apply** command forcibly installs the downloaded update files.

Format

update force apply { **cnc** | **ips-sdb** | **sa-sdb** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cnc	Forcibly installs the malicious domain name database update files.	-
ips-sdb	Forcibly installs the IPS signature database update files.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

Running the **update force apply** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

When you run the **update apply** command to download update files, the update fails in case of insufficient system memory. In this case, you can run the **update force apply** command to forcibly install downloaded update files.

Example

Forcibly install the malicious domain name database update files.

```
<Huawei> system-view
[Huawei] update force apply cnc
```

19.9.1.21 update force local

Function

The **update force local** command configures forcible manual update of local signature database. The signature database is uploaded to the device memory using FTP or SFTP.

Format

update force local { **cnc** | **ips-sdb** | **sa-sdb** } **file** *filename*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cnc	Indicates forcible manual update of the malicious domain name database.	-
ips-sdb	Indicates forcible manual update of the IPS signature database.	-
sa-sdb	Indicates forcible manual update of the SA signature database.	-
file *filename*	Indicates the file used for the update. You must upload the update files to the device memory before the update.	The absolute path of a file is a string of 1 to 64 characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

Running the **update force local** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

When you run the **update local** command to update signature databases locally, the update fails in case of insufficient system memory. In this case, you can run the **update force local** command to forcibly update local signature databases.

Example

Forcibly update the local malicious domain name database using file flash:/cnc_h10010000_2017111500.zip.

```
<Huawei> system-view
[Huawei] update force local cnc file flash:/cnc_h10010000_2017111500.zip
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.1.22 update force online

Function

The **update force online** command forcibly configures the immediate updates of the databases.

Format

update force online { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Forcibly indicates immediate update of the malicious domain name database.	-
ips-sdb	Forcibly indicates immediate update of the IPS signature database.	-
sa-sdb	Forcibly indicates immediate update of the SA signature database.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

Running the **update force online** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

When you run the **update online** command to immediately update signature databases, the update fails in case of insufficient system memory. In this case, you can run the **update force online** command to immediately update signature databases.

Example

Forcibly update the malicious domain name database immediately.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] update force online cnc
```

19.9.1.23 update force restore sdb-default

Function

The **update force restore sdb-default** command forcibly restores the signature database to the factory default version.

Format

update force restore sdb-default { **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
ips-sdb	Forcibly restores the IPS signature database to the factory default version.	-
sa-sdb	Forcibly restores the SA signature database to the factory default version.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

- After you run the **update force restore sdb-default** command, the signature database files corresponding to the rollback version and download version of the signature database will be deleted.
- Running the **update force restore sdb-default** command causes the IAE not to take effect within a short period, resets all IAE-related session tables, and interrupts some services. Therefore, exercise caution when running this command.

When you run the **update restore sdb-default** command to restore the signature database to the default version, the update fails if the system memory is insufficient. In this case, you can attempt to run the **update force restore sdb-default** command to forcibly restore the signature database to the default version.

 Copyright © Huawei Technologies Co., Ltd.

Example

Forcibly restore the IPS signature database to the factory default version.

```
<Huawei> system-view
[Huawei] update force restore sdb-default ips-sdb
```

19.9.1.24 update force rollback

Function

The **update force rollback** command forcibly rolls back the version of a specified database.

Format

update force rollback { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Forcibly rolls back the malicious domain name database version.	-
ips-sdb	Forcibly rolls back the IPS signature database version.	-
sa-sdb	Forcibly rolls back the SA signature database version.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

Running the **update force rollback** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

When you run the **update rollback** command to roll back signature database versions, the update fails in case of insufficient system memory. In this case, you can run the **update force rollback** command to forcibly roll back signature database versions.

 Copyright © Huawei Technologies Co., Ltd.

Example

Forcibly roll back the version of the malicious domain name database.

```
<Huawei> system-view
[Huawei] update force rollback cnc
```

19.9.1.25 update host source

Function

The **update host source** command specifies an interface IP address and VPN instance as the source IP address and VPN instance for online update request packets.

The **update host source ip** command specifies the source IP address of online update request packets.

The **undo update host source** command deletes the specified source IP address and VPN instance and interface of online update request packets.

The **undo update host source ip** command deletes the specified source IP address of online update request packets.

Format

update host source *interface-type interface-number*

update host source ip *ip-address* [**vpn-instance** *vpn-instance*]

undo update host source

undo update host source ip

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and interface number.	-
ip *ip-address*	Specifies the source IP address of online update request packets.	The value is in dotted decimal notation.
vpn-instance *vpn-instance*	Specifies the name of a VPN instance.	The name is a string of 1 to 31 characters.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

In normal cases, these commands are optional. If the administrator does not configure these commands, the system searches a route based on the IP address of the update server and uses the IP address of the outgoing interface as the source IP address of update request packets.

When the Router connects to the Internet through a VPN instance, these commands are mandatory. If the commands are not configured, the update will fail.

- When **update host source** *interface-type interface-number* is configured, the interface must be bound to the corresponding VPN instance name.
- When the **update host source ip** *ip-address* command is configured, **vpn-instance** *vpn-instance* must be specified.

Instructions on these commands are as follows:

- The interface specified in the **update host source** *interface-type interface-number* command is not necessarily the outgoing interface of update request packets. This command actually specifies the IP address of a specific interface as the source IP address. To send update request packets, the system checks the route information to determine the outgoing interface.
- If the interface has multiple IP addresses, run the **update host source ip** *ip-address* command to set the source IP address of update request packets and ensure that the Router can receive the reply packets. Otherwise, the online update may fail.

  The source IP address of the upgrade request packet cannot be the loopback address.
- When both **update host source** *interface-type interface-number* and **update host source ip** *ip-address* [**vpn-instance** *vpn-instance*] are configured, the system preferentially uses the specified IP address as the source IP address of update request packets. That is, the **update host source** *interface-type interface-number* command does not take effect.

Example

Set the interface used for online update to GigabitEthernet1/0/0.

```
<Huawei> system-view
[Huawei] interface GigabitEthernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] update host source GigabitEthernet 1/0/0
```

Set the source IP address of online update request packets to 10.1.1.1.

```
<Huawei> system-view
[Huawei] update host source ip 10.1.1.1
```

19.9.1.26 update local

 Copyright © Huawei Technologies Co., Ltd.

Function

The **update local** command configures manual update of local signature database.

Format

update local { **cnc** | **ips-sdb** | **sa-sdb** } **file** *filename*

Parameters

Parameter	Description	Value
cnc	Indicates the malicious domain name database.	-
ips-sdb	Indicates the IPS signature database.	-
sa-sdb	Indicates the application identification signature database.	-
file *filename*	Specifies the update file. You must upload the update files to the device memory using FTP or SFTP before the update.	The absolute path of a file is a string of 1 to 64 characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

If the device cannot connect to the network, download the update files from the security center (isecurity.huawei.com) to a PC and upload the files to the device memory using FTP or SFTP. Then run the **update local** command to update the databases.

Example

Manually update the local malicious domain name database using file flash:/cnc_h10010000_2017111500.zip.

```
<Huawei> system-view
[Huawei] update local cnc file flash:/cnc_h10010000_2017111500.zip
```

19.9.1.27 update online

 Copyright © Huawei Technologies Co., Ltd.

Function

The **update online** command configures the immediate updates of the databases.

Format

update online { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Indicates the malicious domain name database.	-
ips-sdb	Indicates the IPS signature database.	-
sa-sdb	Indicates the application identification signature database.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The online update modes of signature databases include scheduled update and immediate update. Generally, scheduled update is used. In some case, a signature database needs to be updated to the latest version immediately. If the scheduled update period does not expire, you can run the **update online** command to start immediate update. Before the update, you need to check whether the domain name or IP address of the update center is accessible.

Example

Update the malicious domain name database immediately.

```
<Huawei> system-view
[Huawei] update online cnc
```

19.9.1.28 update online-mode

Function

The **update online-mode** command sets the online update mode of the signature database.

The **undo update online-mode** command restores the default setting.

 Copyright © Huawei Technologies Co., Ltd.

Format

update online-mode { **http** | **https** }

undo update online-mode

Parameters

Parameter	Description	Value
https	Indicates the HTTPS update mode, in which the device uses HTTPS to send update requests and download signature databases.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the online update is in HTTPS mode.

NOTE

Update in HTTP mode is risky, and update in HTTPS mode is recommended. To perform update in HTTP mode, you must strictly restrict security policy matching conditions.

This setting applies only to online update in direct update scenarios (including scheduled update and immediate update) but not online update through a proxy server.

Example

Set the online signature database update mode to HTTP.

```
<Huawei> system-view
[Huawei] update online-mode http
```

19.9.1.29 update proxy

Function

The **update proxy** command sets the IP address or domain name of the proxy server.

The **undo update proxy** command deletes the proxy server setting.

 Copyright © Huawei Technologies Co., Ltd.

Format

update proxy { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*] [**user** *user-name* [**password** *password*]]

undo update proxy

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name of the proxy server.	The value is a string of 1 to 64 characters, spaces not supported.
ip *ip-address*	Specifies the IP address of the proxy server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the proxy server.	The value is an integer ranging from 1 to 65535. The default value is 80.
user *user-name*	Specifies the user name for logging in to the proxy server.	The user name is a string and must have been set on the proxy server. The length of a user name without spaces ranges from 1 to 32 characters. The length of a user name with spaces ranges from 3 to 34 characters. If a user name contains spaces, it must be enclosed with quotation marks (such as "user for test").
password *password*	Specifies the password for logging in to the proxy server.	The password is a string and must be the same as the password corresponding to the user name of the proxy server. • The length of a password without spaces ranges from 1 to 32 characters. The length of a password with spaces ranges from 3 to 34 characters. If a password contains spaces, it must be enclosed with quotation marks. • The password cannot be composed only by asterisks (*).

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None.

Example

Configure a proxy server.

```
<Huawei> system-view
[Huawei] update proxy ip 192.168.2.33 port 8080 user test password Hello!123
```

19.9.1.30 update proxy enable

Function

The **update proxy enable** command enables the signature database proxy update function.

The **undo update proxy enable** command disables the signature database proxy update function.

Format

update proxy enable

undo update proxy enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the signature database proxy update function is disabled.

After this function is enabled, you must run the **update proxy** command to set the proxy server. Otherwise, the firewall cannot connect to the update server through the proxy server.

NOTE

During signature database update through a proxy server, HTTP will be used, causing security risks. You are advised to update the signature database in local or direct update mode.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the signature database proxy update function.

```
<Huawei> system-view
[Huawei] update proxy enable
Info: The proxy function uses the HTTP protocol, which is an unsecured protocol, user name and password plaintext transmission.
```

19.9.1.31 update restore sdb-default

Function

The **update restore sdb-default** command restores the signature database to the factory default version.

Format

update restore sdb-default { **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
ips-sdb	Restores the IPS signature database to the factory default version.	-
sa-sdb	Restores the application identification signature database to the factory default version.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run the **update restore sdb-default** command, the signature database files corresponding to the rollback version and download version of the signature database will be deleted. Therefore, exercise caution when running this command.

Example

Restore the IPS signature database to the factory default version.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] update restore sdb-default ips-sdb
```

19.9.1.32 update rollback

Function

The **update rollback** command rolls back the version of a specified database.

Format

update rollback { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Rolls back the malicious domain name database version.	-
ips-sdb	Rolls back the IPS signature database version.	-
sa-sdb	Rolls back the application identification signature database version.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Run the **update rollback** command to roll back the current version of a specified database to an earlier version. Only one earlier version is available for version rollback. If you run the **update rollback** command a second time, the version of the database is rolled back to the current version again.

NOTE

The version rollback function is unavailable before the second update is complete.

Example

Roll back the version of the malicious domain name database.

```
<Huawei> system-view
[Huawei] update rollback cnc
```

19.9.1.33 update schedule

 Copyright © Huawei Technologies Co., Ltd.

Function

The **update schedule** command sets scheduled update time for the signature database.

Format

update schedule [{ **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time*]

update schedule { **cnc** | **ips-sdb** } { **hourly** *minute* | { **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time* }

update schedule sa-sdb { **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time*

Parameters

Parameter	Description	Value
daily	Indicates daily update of a signature database.	-
weekly { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** }	Indicates weekly update of a signature database.	-
cnc	Indicates scheduled update time of malicious domain name database.	-
ips-sdb	Indicates scheduled update time of IPS-SDB.	-
sa-sdb	Indicates scheduled update time of SA-SDB.	-
hourly	Indicates hourly update of IP reputation database. **NOTE** The AR3260 does not support this parameter.	-
minute	Specifies the minute.	The value ranges from 0 to 59.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time	Specifies the time in a day for the scheduled update of the signature database.	The format is **hh:mm**. The hour and minute are separated by a colon (:). The **hh** value is an integer ranging from 0 to 23 and the **mm** value is an integer ranging from 0 to 59.

Views

System view

Default Level

3: Management level

Usage Guidelines

- Using the **update schedule** command, you can update all signature databases daily at any point during the time range 22:00 to 08:00.
- Using the **update schedule** [{ **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time*] command, you can configure scheduled update time for all signature databases.
- Using the **update schedule** { **cnc** | **ips-sdb** } { **hourly** *minute* | { **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time* } command, you can configure scheduled update time for a signature database.
- Using the **update schedule sa-sdb** { **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time* command, you can configure scheduled update time for the application identification signature database.

Example

Configure a scheduled update of signature databases at 02:00 every Wednesday.

```
<Huawei> system-view
[Huawei] update schedule weekly wed 02:00
```

Configure a scheduled update of signature database at 03:00 every day.

```
<Huawei> system-view
[Huawei] update schedule daily 03:00
```

19.9.1.34 update schedule enable

Function

The **update schedule enable** command enables scheduled update time for the signature database.

 Copyright © Huawei Technologies Co., Ltd.

The **undo update schedule enable** command disables scheduled update time for the signature database.

Format

update schedule { **cnc** | **ips-sdb** | **sa-sdb** } **enable**

undo update schedule { **cnc** | **ips-sdb** | **sa-sdb** } **enable**

Parameters

Parameter	Description	Value
cnc	Indicates the malicious domain name database.	-
ips-sdb	Indicates the IPS signature database.	-
sa-sdb	Indicates the application identification signature database.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, scheduled update time for the signature database is enabled.

Example

Enable the scheduled update time function for the malicious domain name database.

```
<Huawei> system-view
[Huawei] update schedule cnc enable
```

19.9.1.35 update schedule retry-download interval

Function

The **update schedule retry-download interval** command sets the retry interval for downloading the signature database for scheduled update.

The **undo update schedule retry-download interval** command restores the default interval.

Format

update schedule retry-download interval *interval-value*

 Copyright © Huawei Technologies Co., Ltd.

undo update schedule retry-download interval

Parameters

Parameter	Description	Value
interval-value	Specifies the retry interval for downloading the signature database for scheduled update.	The value is an integer ranging from 300 to 3600, in second. The default value is 3600 seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

In case of scheduled update, if the update server is busy, the signature database fails to be download, causing an update failure. Then, the device will retry downloading the signature database. The **update schedule retry-download interval** command is used to set the retry interval for downloading the signature database.

Example

Set the retry interval for downloading the signature database for scheduled update to 1800s.

```
<Huawei> system-view
[Huawei] update schedule retry-download interval 1800
```

19.9.1.36 update schedule retry-load interval

Function

The **update schedule retry-load interval** command sets the retry interval for loading the signature database for scheduled update.

The **undo update schedule retry-load interval** command restores the default interval.

Format

update schedule retry-load interval *interval-value*

undo update schedule retry-load interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval-value	Specifies the retry interval for loading the signature database for scheduled update.	The value is an integer ranging from 300 to 3600, in second. The default value is 3600 seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

In case of scheduled update, if the memory of the device is insufficient, the device fails to load the downloaded signature database. Then, the device will retry loading the signature database. The **update schedule retry-load interval** command is used to set the retry interval for loading the signature database.

Example

Set the retry interval for loading the signature database for scheduled update to 1800s.

```
<Huawei> system-view
[Huawei] update schedule retry-load interval 1800
```

19.9.1.37 update server

Function

The **update server** command sets the IP address or domain name of the update server.

The **undo update server** command deletes the IP address or domain name of the update server.

Format

update server { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*]

undo update server

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name of the update server.	The value is a string of 1 to 64 characters, spaces not supported.
ip *ip-address*	Specifies the IP address of the update server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the update server.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the domain name of the update server is sec.huawei.com, the HTTP port number is 80 and the HTTPS port number is 443.

Example

Set the IP address of the update server to 10.1.1.1 and port number to 86.

```
<Huawei> system-view
[Huawei] update server ip 10.1.1.1 port 86
```

19.9.2 Intrusion Prevention Configuration Commands

NOTE

- The following product models support IPS function:
  - AR160 series: AR169BF, AR169FGW-L, AR169FGVW-L, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169EGW-L, AR169EW, AR168F-4P, AR161EW, AR161EW-M1, AR161FW, AR161FV-1P, and AR169FVW.
  - AR1200 series: AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: AR2204, AR2204XE, AR2204XE-DC, AR2220, AR2220E, AR2240, and AR2240C.
  - AR3200 series: All models.

19.9.2.1 action (IPS signature filter view)

Function

The **action** command configures the action for an IPS signature filter.

 Copyright © Huawei Technologies Co., Ltd.

The **undo action** command restores the default configuration.

Format

action { **alert** | **block** | **default** }

undo action

Parameters

Parameter	Description	Value
alert	Sets the action to **alert**. The device permits packets and generates a log when the packets match a signature in the signature filter.	-
block	Sets the action to **block**. The device discards packets and generates a log when the packets match a signature in the signature filter.	-
default	Uses the default action.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

The default action for the signature filter is **default**. That is, when a packet matches a signature in the signature filter, the device performs the action for the signature.

After you set the action for the signature filter to **alert** or **block**, the actions for the signatures in the signature filter no longer take effect. When packets match a signature in the signature filter, the device performs the action for the signature filter.

Example

Set the action for IPS signature filter **hello** to **alert**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] action alert
```

19.9.2.2 action (user-defined IPS signature view)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **action** command configures the action for a user-defined signature.

The **undo action** command restores the default configuration.

Format

action { **alert** | **block** | **allow** }

undo action

Parameters

Parameter	Description	Value
alert	Sets the action to **alert**. The device permits packets and generates a log when the packets match the signature.	-
block	Sets the action to **block**. The device discards packets and generates a log when the packets match the signature.	-
allow	Sets the action to **allow**. The device permits packets when the packets match the signature.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

If a signature is referenced in a signature filter, the action for the signature filter applies if packets match the signature.

The default action for the signature is **alert**.

Example

Configure a user-defined signature. Set the ID to **1**, name to **mysignature**, and action to **block**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
[Huawei-ips-signature-1] action block
```

19.9.2.3 application (IPS signature filter view)

Function

The **application** command configures an application name in an IPS signature filter.

 Copyright © Huawei Technologies Co., Ltd.

The **undo application** command removes the configured application name.

Format

application { *application-name* &<1-10> | **all** }

undo application { *application-name* &<1-10> | **all** }

Parameters

Parameter	Description	Value
application-name &<1-10>	Specifies the name of the application. A maximum of 10 application names can be specified.	-
all	Indicates all applications.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

The application name specified in this command is a filtering condition in the IPS signature filter and helps filter packets of the specified application.

&<1-10> indicates that a maximum of 10 applications can be specified at a time. To specify more applications, repeat this command. A packet matches the filtering condition if the application type of this packet matches any of the specified applications.

If no application is specified, the IPS does not filter packets based on application names.

Example

In IPS profile **profile1**, configure **example_application** as the filtering condition in IPS signature filter **hello**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] application example_application
```

19.9.2.4 assoc-check enable

 Copyright © Huawei Technologies Co., Ltd.

Function

The **assoc-check enable** command enables the correlation detection function.

The **undo assoc-check enable** command disables the correlation detection function.

Format

assoc-check enable

undo assoc-check enable

Parameters

None

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, the function is enabled.

Intrusion prevention detects traffic by signatures that can be either basic signatures or correlation signatures. A basic signature describes a simple network attack. A correlation signature is composed of one or more basic signatures and describes a complex network attack. Correlation detection is implemented on the basis of correlation signatures.

If traffic matches a correlation signature, the system displays only the matched correlation signature, but not the matched basic signature of the correlation signature. After the correlation detection function is disabled, when traffic matches a basic signature included in a correlation signature, the system displays the basic signature.

Disabling correlation detection decreases the security detection capability of the system and therefore is not recommended. In addition, it is easy for traffic to match a basic signature included in a correlation signature. Therefore, correlation detection deteriorates the device performance.

Example

Enable correlation detection in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] assoc-check enable
```

19.9.2.5 category (IPS signature filter view)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **category** command adds the Intrusion Prevention System (IPS) signature of the specified category to an IPS signature filter.

The **undo category** command deletes the IPS signature of the specified category from an IPS signature filter.

Format

category { *category-name* &<1-10> | **all** }

undo category { *category-name* &<1-10> | **all** }

Parameters

Parameter	Description	Value
category-name &<1-10>	Specifies the category name. **&<1-10>** indicates that a command can have 1 to 10 such parameter values.	-
all	Indicates all categories.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

You can add signatures of a maximum of 10 categories to the signature filter at a time. To add signatures of more categories, repeat this command.

Signature categories may vary with IPS signature files. After you update the IPS signature database, view the changes of signature categories and modify configurations accordingly.

NOTE

When the IPS signature database is not loaded, only parameter **all** is available.

Example

Configure category **Remote-File-Inclusion** for IPS signature filter **hello** in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] category Remote-File-Inclusion
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.6 check (user-defined signature rule view)

Function

The **check** command configures the matching order of user-defined signature rules.

The **undo check** command restores the default configuration.

Format

check { **sequential** | **random-order** }

undo check

Parameters

Parameter	Description	Value
sequential	Indicates that user-defined signature rules are matched sequentially.	-
random-order	Indicates that user-defined signature rules are matched in random order.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

User-defined signature rules are matched in random order by default.

If you select **sequential**, conditions are matched in ascending order by ID. An intrusion matches a rule only when the intrusion matches all conditions of the rule in configuration order.

If you select **random-order**, conditions are matched in random order. An intrusion matches a rule when the intrusion matches all conditions of the rule in either configuration order or random order.

NOTE

Selecting **sequential** is not recommended. If you select it, the matching order becomes stricter, which may cause false positives during intrusion detection. Sequential check does not apply to value match (including:equal, gthan, lthan, and noequal).

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the matching order to **sequential**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] check sequential
```

19.9.2.7 cnc domain-filter enable

Function

The **cnc domain-filter enable** command enables the domain name-based filtering function.

The **undo cnc domain-filter enable** command disables the domain name-based filtering function.

Format

cnc domain-filter enable [**action** { **alert** | **block** }]

undo cnc domain-filter enable

Parameters

Parameter	Description	Value
action	Indicates the action.	-
alert	Indicates that the device permits packets matching a malicious domain name, but generates an alarm and logs the event.	-
block	Indicates that the device discards packets matching a malicious domain name and logs the event.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, domain name-based filtering is disabled.

After domain name-based filtering is enabled, the default action is **alert** for packets matching the specified condition. After running **cnc domain-filter enable** to enable the function or **undo cnc domain-filter enable** to disable the function, run **engine configuration commit** to commit the configuration change to apply it.

 Copyright © Huawei Technologies Co., Ltd.

The domain name-based filtering function enables the device to filter out packets using the malicious domain name signature database. Upon receiving a packet matching a malicious domain name, the device implements the specified action and logs the threats for auditing and troubleshooting.

Example

In IPS profile **profile1**, enable domain name-based filtering and set **action** to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] cnc domain-filter enable action block
[Huawei-profile-ips-profile1] quit
[Huawei] engine configuration commit
```

19.9.2.8 cnc domain-filter exception domain-name

Function

The **cnc domain-filter exception domain-name** command adds an exception domain name.

The **undo cnc domain-filter exception domain-name** command deletes an exception domain name.

Format

cnc domain-filter exception domain-name *domain-name*

undo cnc domain-filter exception { **domain-name** *domain-name* | **all** }

Parameters

Parameter	Description	Value
domain-name	Specifies a malicious domain name.	The value is a string of 4 to 255 characters.
all	Indicates all malicious domain names.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

These commands are used to add or delete exception domain names. To view all specified exception domain names, run **display cnc domain-filter exception**.

The exception domain name must be a domain name in the malicious domain name signature database. Adding any domain name that is not in the malicious domain name signature database is pointless. You can determine whether to add a malicious domain name as an exception domain name based on the threat logs. After a malicious domain name is added as an exception domain name, the device does not filter out the packets matching the exception domain name.

Example

Add **www.example.com** as an exception domain name.

```
<Huawei> system-view
[Huawei] cnc domain-filter exception domain-name www.example.com
```

Delete all exception domain names.

```
[Huawei] undo cnc domain-filter exception all
```

19.9.2.9 collect-attack-evidence enable (intrusion prevention profile view)

Function

The **collect-attack-evidence enable** command enables attack evidence collection of intrusion prevention.

The **undo collect-attack-evidence enable** command disables attack evidence collection of intrusion prevention.

Format

collect-attack-evidence enable

undo collect-attack-evidence enable

Parameters

None

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

The attack evidence collection function of intrusion prevention is disabled by default.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Attack evidence collection does not apply to HTTPS traffic.
- Attack evidence collection is for troubleshooting only. Because attack evidence collection compromises system performance, you must enable it only when necessary and disable it immediately after you finish attack evidence collection.

After you enable the attack evidence collection function, the device starts to collect the packets that match the intrusion prevention profile. If the action in the intrusion prevention profile is block, the device collects only the identified threat packets and previous packets. Subsequent packets of the same session are blocked and discarded by the device, and therefore are not collected. If the action in the intrusion prevention profile is not block, the device collects all threat packets of the session.

One of the extreme conditions is that: The action in the intrusion prevention profile is not block and the device collects the packets that match the intrusion prevention profile. However, the storage space is insufficient after the device collects some threat packets. As a result, the device stops attack evidence collection.

Example

Enable attack evidence collection in intrusion prevention profile **hello**.

```
<Huawei> system-view
[Huawei] profile type ips name hello
[Huawei-profile-ips-hello] collect-attack-evidence enable
```

19.9.2.10 condition (user-defined signature rule view)

Function

The **condition** command configures a matching condition of a user-defined signature rule.

The **undo condition** command deletes a matching condition from a user-defined signature rule.

Format

condition [*condition-id*] **field** *field-name* **operate** { **equal** | **gthan** | **lthan** | **noequal** } **value** *value-content* [**direction** *direction* | **qualifier http-method** *http-method*] *

condition [*condition-id*] **field** *field-name* **operate pmatch value** *value-content* [**offset** { *offset-value* | **begin** }] [**depth** *depth-value*] [**direction** *direction* | **qualifier http-method** *http-method*] *

undo condition { *condition-id* | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
condition-id	Specifies the ID of a condition.	The value is an integer ranging from 1 to 4.
field *field-name*	Specify a protocol field to be checked.	After you run the **protocol** command in the user-defined IPS signature view, you can check the field of the specified protocol. The default protocol of a user-defined signature is HTTP. Therefore, the *field-name* is the HTTP protocol field.
operate { **equal** | **gthan** | **lthan** | **noequal** }	Indicates the comparison action.	• **equal** indicates that the value of *field-name* equals to the value of *value-content*. • **gthan** indicates that the value of *field-name* is greater than the value of *value-content*. • **lthan** indicates that the value of *field-name* is less than the value of *value-content*. • **noequal** indicates that the value of *field-name* does not equal to the value of *value-content*.
value *value-content*	Specifies the field value.	• If you set *field-name* to **DNS.RR.A.Address**, the value is an IPv4 address in dotted decimal notation. • If you set *field-name* to **MSRPC.Interface**, the value is a hexadecimal string of 32 characters. • If you set *field-name* to other value: – If you set **operate** to **pmatch**, the value is a string of 7 to 127 characters. If the keyword contains any space and question mark (?), the value is a string of 9 to 129 characters and must be enclosed with double quotation marks (""), for example, "abcd wd?". If the keyword contains quotation marks, replace the quotation marks with \x22, for example, to set keyword **abc"ddd**, enter **abc \x22ddd**. – If you set **operate** to another value, the value is an integer ranging from 0 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
operate pmatch	Sets the comparison action to pattern matching.	If the *field-name* field contains the *value-content* string, the condition is matched.
offset *offset-value*	Specifies the offset of pattern matching.	The value is an integer ranging from 0 to 65535. The default value is 0, indicating that a match is searched for from the start location of the *field-name* field. As long as a match of the *value-content* value is found in the *depth-value* range, the user-defined signature rule is matched. When the *offset-value* is 1, a match is searched for from the second byte of the *field-name* field. As long as a match of the *value-content* value is found in the *depth-value* range, the user-defined signature rule is matched. • If *field-name* is set to **MSRPC.Interface**, the **offset** *offset-value* parameter cannot be specified. • If *field-name* is not set to **MSRPC.Interface** and **operate** is not **pmatch**, the **offset** *offset-value* parameter cannot be specified. • If *field-name* is not set to **MSRPC.Interface** but **operate** is **pmatch**, the **offset** *offset-value* parameter can be specified.
begin	Implements pattern match from the start location of the *field-name* field. The user-defined signature rule is matched only when a match of the *value-content* value is found.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
depth *depth-value*	Specifies the depth of pattern matching.	The value is an integer ranging from 7 to 65535. The value of *depth-value* must be greater than the number of characters in *value-content*. If *offset-value* is 1 and *depth-value* is 10, the matching starts from the second byte of the *field-name* field and 10 bytes will be matched. The matching succeeds as long as the *value-content* is within the specified range. • If *field-name* is set to **MSRPC.Interface**, the **depth** *depth-value* parameter cannot be specified. • If *field-name* is not set to **MSRPC.Interface** and **operate** is not **pmatch**, the **depth** *depth-value* parameter cannot be specified. • If *field-name* is not set to **MSRPC.Interface** but **operate** is **pmatch**, the **depth** *depth-value* parameter can be specified.
direction *direction*	Specifies the packet check direction.	The direction can be: • **both** Packets from the client and server are checked. • **from-client** Packets from the client are checked. • **from-server** Packets from the server are checked. **both** is the default configuration, and packets from the client and server are checked.
qualifier	Indicates the qualifier information.	-
http-method *http-method*	Checks the **Method** field of HTTP.	Supported HTTP methods include **GET**, **POST**, **PUT**, **HEAD**, **DELETE**, **OPTIONS**, **CONNECT**, **TRACE**, **LINK**, **UNLINK**, **PATCH**, **MOVE**, **COPY**, **WRAPPED**, **PROFIND**, and **PROPPATCH**. As for user-defined signature rule check items, you can configure only one HTTP Method check item and only one method.
all	Indicates all conditions.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

If *condition-id* is not specified, the system automatically sets the IDs to the missing numbers in ascending order. For example, conditions **1**, **3**, and **4** already exist in the system, and another condition is created but the *condition-id* is not specified. In this case, the system automatically sets the ID of the new condition to **2**.

Example

Create user-defined signature rule **hello** in user-defined signature **1**. Configure condition **1** to check field **HTTP.Authorization** whose value matches **threat_string**, and condition **2** to check field **HTTP.Content-Length** whose value is equal to **111**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol HTTP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] condition 1 field HTTP.Authorization operate pmatch value threat_string
[Huawei-ips-signature-1-rule-hello] condition 2 field HTTP.Content-Length operate equal value 111
```

Create user-defined signature rule **hello** in user-defined signature **2**. Configure condition **1** to check the **HTTP.Authorization** field that matches **threat_string** and set the offset to **1** and depth to **10**.

```
<Huawei> system-view
[Huawei] ips signature-id 2
[Huawei-ips-signature-2] protocol HTTP
[Huawei-ips-signature-2] rule name hello
[Huawei-ips-signature-2-rule-hello] condition 1 field HTTP.Authorization operate pmatch value threat_string offset 1 depth 10
```

19.9.2.11 condition associated (user-defined signature rule view)

Function

The **condition associated** command sets a check item for a user-defined associated signature.

The **undo condition associated** command cancels the settings of the check item for a user-defined associated signature.

Format

condition associated signature-id *signature-id* [**threshold** *threshold-value* | **interval** *interval-value* | **correlateby** { **source** | **destination** | **source-destination** }] *

 Copyright © Huawei Technologies Co., Ltd.

undo condition associated

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies an associated signature ID. The value can be the ID of a user-defined or predefined signature, but cannot be the ID of a user-defined or predefined associated signature. The associated signature and user-defined associated signature must use the same protocol and object information.	The value is an integer ranging from 1 to 16777215.
threshold *threshold-value*	Specifies the threshold for signature association times.	The value is an integer ranging from 1 to 500. The default value is 30.
interval *interval-value*	Specifies the measurement period. If the number of times the associated signature is detected exceeds *threshold-value* within this period, the user-defined associated signature is matched.	The value is an integer ranging from 1 to 7200. The default value is 60.
correlateby	Indicates the association mode.	The default mode is **source-destination**.
source	Counts the times the associated signature is matched based on source IP addresses.	-
destination	Counts the times the associated signature is matched based on destination IP addresses.	-
source-destination	Counts the times the associated signature is matched based on a pair of source and destination IP addresses.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

Only one rule can be configured for a user-defined associated signature. Only one check item can be configured in the rule.

 Copyright © Huawei Technologies Co., Ltd.

If a user-defined signature is configured as an associated signature, you must remove the association relationship of the signature before deleting the user-defined signature. Only enabled predefined signatures can be configured as associated signatures.

During the IPS signature database update, if the associated signature configured for correlation detection does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

Example

Configure a check item for a user-defined associated signature.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] rule name rule1
[Huawei-ips-signature-1-rule-rule1] condition associated signature-id 1000 threshold 20 interval 23 correlateby source-destination
```

19.9.2.12 condition move (user-defined signature rule view)

Function

The **condition move** command moves a condition of the specified user-defined signature rule.

Format

condition move *condition-id* **to** *new-condition-id*

Parameters

Parameter	Description	Value
condition-id	Specifies the ID of the condition to be moved in the specified user-defined signature rule.	The value is an integer ranging from 1 to 4.
new-condition-id	Specifies the destination position (new ID of the condition) of the moved condition in the user-defined signature rule.	The value is an integer ranging from 1 to 4.

Views

User-defined signature rule view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After you run the **check** command to configure the matching order of conditions in a user-defined signature rule to **sequential**, you can move the condition to change its priority.

If the destination *new-condition-id* is used by a condition, the moved condition and the owner of the destination ID switch IDs. For example, conditions **1** to **4** exist in a user-defined signature rule. When you run the **condition move 4 to 1** command to move condition **4** to the position of condition **1**, condition **4** becomes condition **1**, and the original condition **1** becomes condition **4**.

Example

View the existing conditions in user-defined signature rule **hello**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol HTTP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] display this
#
 condition 1 field HTTP.HeadContent operate pmatch value abcdabcd
 #
 condition 2 field HTTP.Content-Type operate pmatch value efghefgh
 #
 condition 3 field HTTP.Transfer-Encoding operate pmatch value ijklijkl
#
return
```

Move condition **2** in the user-defined signature rule to the position of condition **4**, and view the result of the move.

```
[Huawei-ips-signature-1-rule-hello] condition move 2 to 4
[Huawei-ips-signature-1-rule-hello] display this
#
 condition 1 field HTTP.HeadContent operate pmatch value abcdabcd
 #
 condition 3 field HTTP.Transfer-Encoding operate pmatch value ijklijkl
 #
 condition 4 field HTTP.Content-Type operate pmatch value efghefgh
#
return
```

Move condition **4** in the user-defined signature rule to the position of condition **1**, and view the result of the move.

```
[Huawei-ips-signature-1-rule-hello] condition move 4 to 1
[Huawei-ips-signature-1-rule-hello] display this
#
 condition 1 field HTTP.Content-Type operate pmatch value efghefgh
 #
 condition 3 field HTTP.Transfer-Encoding operate pmatch value ijklijkl
 #
 condition 4 field HTTP.HeadContent operate pmatch value abcdabcd
#
return
```

19.9.2.13 context-awareness enable

Function

The **context-awareness enable** command enables context awareness.

 Copyright © Huawei Technologies Co., Ltd.

The **undo context-awareness enable** command disables context awareness.

Format

context-awareness { **all** | **http** | **os** } **enable**

undo context-awareness { **all** | **http** | **os** } **enable**

Parameters

Parameter	Description	Value
all	Indicates all awareness functions.	-
http	Indicates the HTTP application awareness function.	-
os	Indicates the operating system awareness function.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the device to detect HTTP applications or operating systems on the network, enable context awareness.

By default, context awareness is disabled.

Example

Enable the operating system awareness function.

```
<Huawei> system-view
[Huawei] context-awareness os enable
```

19.9.2.14 description (intrusion prevention profile view)

Function

The **description** command configures the description of an intrusion prevention profile.

The **undo description** command deletes the description of an intrusion prevention profile.

 Copyright © Huawei Technologies Co., Ltd.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an intrusion prevention profile.	The value is a case-sensitive string of 1 to 128 characters. Spaces are supported.

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

You are advised to describe the features of each intrusion prevention profile.

Example

Configure description **HTTP protocol and windows system** for intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] description HTTP protocol and windows system
```

19.9.2.15 description (user-defined IPS signature view)

Function

The **description** command configures the description of a user-defined signature.

The **undo description** command deletes the description of a user-defined signature.

Format

description *description*

undo description

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
description	Specifies the description of a user-defined signature.	The value is a case-sensitive string of 1 to 128 characters. Spaces are supported.

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

You are advised to describe the features of each user-defined signature.

Example

Configure a user-defined signature. Set the ID to **1**, name to **mysignature**, and description to **HTTP protocol and targeting client**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
[Huawei-ips-signature-1] description HTTP protocol and targeting client
```

19.9.2.16 destination-ip (user-defined signature rule view)

Function

The **destination-ip** command specifies the destination IP address to be checked by a user-defined signature rule.

The **undo destination-ip** command deletes the destination IP address to be checked by a user-defined signature rule.

Format

destination-ip { [**ipv4**] *start-ipv4-address* [*end-ipv4-address* | *ipv4-mask-length*] | **any** }

undo destination-ip

Parameters

Parameter	Description	Value
start-ipv4-address	Specifies the start IPv4 address.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end-ipv4-address	Specifies the end IPv4 address.	The value is in dotted decimal notation.
ipv4-mask-length	Specifies the mask length of the IPv4 address.	The value is an integer ranging from 1 to 32.
any	Indicates any IP address.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

All destination IP addresses are checked by the user-defined signature rule by default.

The user-defined signature rule can be used to check a single IP address or all address in an IP address range. To use a user-defined signature rule to check an IP address range, you can specify the start and end IP addresses or the mask-length to define the IP address range.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the destination IPv4 address to be checked to **10.2.2.1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] destination-ip 10.2.2.1
```

In user-defined signature with the ID of 1, specify user-defined signature rule **hello** and set the destination IP address range from **10.2.2.1** to **10.2.2.100** to be checked.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] destination-ip 10.2.2.1 10.2.2.100
```

19.9.2.17 destination-port (user-defined signature rule view)

Function

The **destination-port** command specifies the destination port to be checked by a user-defined signature rule.

 Copyright © Huawei Technologies Co., Ltd.

The **undo destination-port** command deletes the destination port to be checked by a user-defined signature rule.

Format

destination-port { *start-port end-port* | **any** }

undo destination-port

Parameters

Parameter	Description	Value
start-port	Specifies the start port of a port range to be checked by the user-defined signature rule.	The value is an integer ranging from 1 to 65535.
end-port	Specifies the end port of a port range to be checked by the user-defined signature rule.	The value is an integer ranging from 1 to 65535. The value of *end-port* must be no smaller than that of *start-port*.
any	Indicates that all destination ports are checked by the user-defined signature rule.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

All destination ports are checked by the user-defined signature rule by default.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the destination port range to a range from **80** to **8080**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] destination-port 80 8080
```

19.9.2.18 display cnc domain-filter domain statistics

 Copyright © Huawei Technologies Co., Ltd.

Function

The **display cnc domain-filter domain statistics** command displays the top N matched malicious domain names.

Format

display cnc domain-filter domain statistics [*topn-number*]

Parameters

Parameter	Description	Value
topn-number	Specifies how many most matched malicious domain names are displayed.	The value is an integer ranging from 1 to 50.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the top N matched malicious domain names.

Example

Display the top 10 matched malicious domain names.

```
<Huawei> display cnc domain-filter domain statistics 10
 Domain statistics topN on slot 0 cpu 0:
 ------------------------------------------------------------------------------
 *                        TOP-N Statistics                      *
 *                        (Counts:   10)                        *
 ------------------------------------------------------------------------------
 TOP-N Domain Name                                          Event Counts
 ------------------------------------------------------------------------------
 1    www.example1.com                                        20
 2    www.example2.com                                        19
 3    www.example3.com                                        18
 4    www.example4.com                                        17
 5    www.example5.com                                        16
 6    www.example6.com                                        15
 7    www.example7.com                                        14
 8    www.example8.com                                        13
 9    www.example9.com                                        12
 10    www.example10.com                                       11
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-103 Description of the **display cnc domain-filter domain statistics** command output

Item	Description
TOP-N Statistics	Statistics on top N malicious domain names
Counts	Value of N
TOP-N Domain Name	Top N malicious domain names
Event Counts	Number of events

19.9.2.19 display cnc domain-filter exception

Function

The **display cnc domain-filter exception** command displays all exception domain names.

Format

display cnc domain-filter exception

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After using the **cnc domain-filter exception domain-name** command to add or delete exception domain names, you can run the command to view all configured exception domain names.

Example

Display all exception domain names.

```
<Huawei> display cnc domain-filter exception
 domain-filter exception-domain:
 Counts: 1
 ------------------------------------------------------------
 domain-name
 ------------------------------------------------------------
 www.example.com
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-104 Description of the **display cnc domain-filter exception** command output

Item	Description
domain-filter exception-domain	Exception domain name in domain name-based filtering
Counts	Number of exception domain names
domain-name	Exception domain name

19.9.2.20 display cnc domain-filter statistics

Function

The **display cnc domain-filter statistics** command displays domain name filtering statistics.

Format

display cnc domain-filter { **exception** | **domain-name** *domain-name* } **statistics**

Parameters

Parameter	Description	Value
exception	Indicates the exception domain name.	-
domain-name	Specifies a malicious or exception domain name.	The value is a string of 4 to 255 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays filtering statistics of a domain name (**domain-name** *domain-name*) or a set of domain names (**exception**). To clear domain name-based filtering statistics, run **19.9.2.59 reset cnc domain-filter statistics**.

Example

Display filtering statistics on malicious domain name **www.example.com**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display cnc domain-filter domain-name www.example.com statistics

--------------------------------------------------------------------------------
Domain Name                                                      Event Counts
--------------------------------------------------------------------------------
www.example1.com                                                 1
```

Table 19-105 Description of the **display cnc domain-filter domain-name** *domain-name* **statistics** command output

Item	Description
Domain Name	Malicious domain name
Event Counts	Number of events

19.9.2.21 display context-awareness information statistics

Function

The **display context-awareness information statistics** command displays the identification results of the context awareness function.

Format

display context-awareness information [**host** *ip-address*] [**http-client** | **http-server** | **os**] **statistics**

Parameters

Parameter	Description	Value
host *ip-address*	Displays identification results by an IPv4 address.	The value is in dotted decimal notation.
http-client	Displays identification results by the HTTP client application.	-
http-server	Displays identification results by the HTTP server application.	-
os	Displays the identification results by the OS.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The context awareness function records the identification results of only IPv4 traffic.

Example

Display the identification results of content awareness.

```
<Huawei> display context-awareness information statistics
------------------------------------------------------------------------------
context-awareness information on slot 11 cpu 0:
------------------------------------------------------------------------------
Address         Dir     OS                          HTTP-Application
10.1.1.1        client  Linux 2.2.x-3.x               Chrome
10.2.1.1        server  Linux 2.2.x-3.x                Apache 1.x
10.3.1.1        server  Other
10.4.1.1        client  Linux 2.2.x-3.x               Safari 5.1 or newer
------------------------------------------------------------------------------
```

Table 19-106 Description of the **display context-awareness information statistics** command output

Item	Description
context-awareness information on slot *X* cpu *Y*	Statistics on CPU *Y* in slot *X*
Address	IPv4 address of the client or server
Dir	Detection direction: • client: traffic from the client • server: traffic from the server
OS	OS of the client or server
HTTP-Application	HTTP application used by the client or server

19.9.2.22 display context-awareness statistics

Function

The **display context-awareness statistics** command displays traffic statistics of different categories by context awareness.

Format

display context-awareness [**http-client** | **http-server** | **os**] **statistics**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
http-client	Indicates an HTTP client application.	-
http-server	Indicates an HTTP server application.	-
os	Indicates the OS.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display traffic statistics by OS by context awareness.

```
<Huawei> system-view
[Huawei] display context-awareness os statistics
------------------------------------------------------------------------------
OS statistic on slot 11 cpu 0:
------------------------------------------------------------------------------
OS                              Count
Android                           68205
Linux 3.x                        114939
Linux 2.6.x                      337404
Linux 2.4.x-2.6.x                125654
Linux 2.2.x-3.x                 1993419
Windows_XP                         6524058
Windows_7,Windows_8                 960383
Windows_7                          0
Mac_OS_X 10.x                       31457
iPhone,iPad                      174576
Mac_OS_X                          936
Other                           1647545
------------------------------------------------------------------------------
```

Table 19-107 Description of the **display context-awareness os statistics** command output

Item	Description
OS statistic on slot *X* cpu *Y*	Statistics on CPU *Y* in slot *X*
OS	OS
Count	Matching count

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.23 display decoding statistics

Function

The **display decoding statistics** command displays decoding statistics.

NOTE

Only the AR160 (except AR169RW-P-M9) support this command.

Format

display decoding statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays decoding statistics.

Example

Display decoding statistics.

```
<Huawei> display decoding statistics
Decoding Statistic Table
------------------------------------------------------------------------------
 Traffic statistic:
------------------------------------------------------------------------------
  Total Traffic  :                    0
------------------------------------------------------------------------------
  Application                 Traffic
------------------------------------------------------------------------------
  HTTP                         0
  FTP                         0
  SMTP                         0
  POP3                         0
  NFS                         0
  SMB                          0
  IMAP                         0
  OTHER                          0
------------------------------------------------------------------------------

 File statistic:
------------------------------------------------------------------------------
  Total File  :                    0
------------------------------------------------------------------------------
  Application                 File
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
  HTTP                          0
  FTP                         0
  SMTP                          0
  POP3                          0
  NFS                         0
  SMB                           0
  IMAP                          0
  OTHER                           0
------------------------------------------------------------------------------
```

19.9.2.24 display ips signature-id rule

Function

The **display ips signature-id rule** command displays the user-defined signature rule with the specified name.

Format

display ips signature-id *signature-id* **rule** { **name** *rule-name* | **all** }

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies the ID of a user-defined signature.	The value is a string of 1 to 1024 characters. The value must be the ID of an existing user-defined signature.
name *rule-name*	Specifies the name of a user-defined signature rule.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-). The value must be the name of an existing user-defined signature rule.
all	Indicates IDs of all user-defined signatures.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display rules of user-defined signature **11**.

```
<Huawei> system-view
[Huawei] display ips signature-id 11 rule name rule1
 IPS Signature Rule Configurations:
 SignatureID      : 11
 ----------------------------------------------------------
  Name            : rule1
  Scope           : flow
  Check           : sequential
  SourceIP        : 10.1.1.1/24
  SourcePort      : 2003-2004
  DestinationIP   :
  DestinationPort : any

  Condition:
    ID   Operator   Field                          Value
  ------------------------------------------------------------
     1   noequal    HTTP.Content-Length              24
  ------------------------------------------------------------
 ------------------------------------------------------------------------
```

Display the user-defined associated signature whose user-defined signature ID is 1.

Table 19-108 Description of the **display ips signature-id rule name** command output

Item	Description
SignatureID	ID of the user-defined signature where the rule reside
Name	Name of a user-defined signature rule
Scope	Detection scope of a user-defined signature rule
Check	Matching order of a user-defined signature rule
SourceIP	Source IP address checked by a user-defined signature rule
SourcePort	Source port checked by a user-defined signature rule
DestinationIP	Destination IP address checked by a user-defined signature rule
DestinationPort	Destination port checked by a user-defined signature rule
Condition	Condition of a user-defined signature rule

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ID	Condition ID
Operator	Field operation of a condition
Field	Field to be checked by a condition
Value	Value of the field to be checked by a condition
Signature-id	ID of the associated signature
ThresholdValue	Threshold for signature association times
IntervalTime	Measurement period
Correlateby	Association mode

19.9.2.25 display ips signature-state

Function

The **display ips signature-state** command displays the state of predefined signatures.

Format

display ips signature-state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Enable all predefined signatures, disable predefined signature 12345, and then commit the changes. After that, disable predefined signature 54330 without committing the change. Then, view the state of all predefined signatures.

```
<Huawei> system-view
[Huawei] ips signature-state enabled
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] ips signature-state signature-id 12345 disabled
[Huawei] engine configuration commit
[Huawei] ips signature-state signature-id 54330 disabled
[Huawei] display ips signature-state
------------------------------------------------------------------
Global    : enabled
Count     : 2
Committed : not committed
------------------------------------------------------------------
Signature-ID    Configured-State    Default-State    Committed
------------------------------------------------------------------
54330           disabled            enabled          not committed
12345           disabled            enabled          committed
```

Table 19-109 Description of the **display ips signature-state** command output

Item	Description
Global	Default state for all predefined signatures can be either of the following: • **enabled**: Predefined signatures are enabled by default. • **disabled**: Predefined signatures are disabled by default. • **non-configured**: The default state of predefined signatures is not configured. To set the default state for all predefined signatures, run **ips signature-state** { **enabled** | **disabled** }. If the default state is not specified, the state will be **non-configured**.
Count	Number of predefined signatures with changed state
Committed	Whether all state changes are committed: • **committed**: All state changes are committed. • **not committed**: Not all state changes are committed.
Signature-ID	ID of a predefined signature.
Configured-State	New state of a predefined signature: • **enabled**: A predefined signature is enabled. • **disabled**: A predefined signature is disabled. To change the state of a predefined signature, run **ips signature-state signature-id** *signature-id* { **enabled** | **disabled** }.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default-State	State of predefined signatures in the IPS signature database: ● **enabled**: A predefined signature is enabled. ● **disabled**: A predefined signature is disabled. ● **retired**: A predefined signature is deprecated. A predefined signature marked with retired is deprecated and retained only for checking the history of signatures.
Committed	Whether the state change of a predefined signature is committed: ● **committed**: The state change is committed. ● **not committed**: The state change is not committed.

19.9.2.26 display ips statistics

Function

The **display ips statistics** command displays IPS statistics.

Format

display ips statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display IPS statistics.

```
<Huawei> display ips statistics
IPS Statistic Table
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
Event statistic:
------------------------------------------------------------------------------
  Total Alert Events  :                  0
  Total Block Events  :                  0
------------------------------------------------------------------------------
  Application             Alert Events             Block Events
------------------------------------------------------------------------------
  HTTP                           0                        0
  FTP                            0                        0
  SMTP                           0                        0
  POP3                           0                        0
  NFS                            0                        0
  SMB                            0                        0
  IMAP                           0                        0
  OTHER                          0                        0
------------------------------------------------------------------------------

Traffic statistic:
------------------------------------------------------------------------------
  Total Traffic  :                       0
------------------------------------------------------------------------------
  Application                Traffic
------------------------------------------------------------------------------
  HTTP                           0
  FTP                            0
  SMTP                           0
  POP3                           0
  NFS                            0
  SMB                            0
  IMAP                           0
  OTHER                          0
------------------------------------------------------------------------------

File statistic:
------------------------------------------------------------------------------
  Total File  :                          0
------------------------------------------------------------------------------
  Application                File
------------------------------------------------------------------------------
  HTTP                           0
  FTP                            0
  SMTP                           0
  POP3                           0
  NFS                            0
  SMB                            0
  IMAP                           0
  OTHER                          0
------------------------------------------------------------------------------
```

19.9.2.27 display ips-signature

Function

The **display ips-signature** command displays information about an IPS signature.

Format

display ips-signature *ips-signature-id*

display ips-signature [{ **pre-defined** | **user-defined** } [**associated**]] [**application** { *application-name* | **all** } | **category** { *category-name* | **all** } | **os** { **all** | **android** | **ios** | **unix-like** | **windows** | **other** } * | **protocol** { *protocol-name* | **all** } | **severity** { **information** | **low** | **medium** | **high** } * | **state** { **disabled** | **enabled** | **retired** } | **target** { **server** | **client** | **both** }] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ips-signature-id	Specifies the ID of an IPS signature.	The value is an integer ranging from 1 to 16777215. The value must be the ID of an existing IPS signature.
pre-defined	Displays information about a predefined signature.	-
user-defined	Displays information about a user-defined signature.	-
associated	Displays information about a associated signature.	-
application { *application-name* | **all** }	Specifies an application name.	• *application-name*: displays information about signatures in application *application-name*. • **all**: displays information about signatures in all applications.
category { *category-name* | **all** }	Displays signatures by category.	• *category-name*: displays information about signatures in category *category-name*. • **all**: displays information about signatures in all categories.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
os { **all** | **android** | **ios** | **unix-like** | **windows** | **other** } *	Displays signatures by operating system.	• **all**: displays information about all signatures. • **android**: displays information about signatures for the Android operating system. • **ios**: displays information about signatures for the iOS operating system. • **unix**: displays information about signatures for the UNIX operating system. • **windows**: displays information about signatures for the Windows operating system. • **other**: displays information about signatures for other operating systems.
protocol { *protocol-name* | **all** }	Displays signatures by protocol.	• *protocol-name*: displays information about signatures of protocol *protocol-name*. • **all**: displays information about signatures of all protocols.
severity { **information** | **low** | **medium** | **high** }*	Displays signatures by severity.	• **information**: displays information about signatures with informational severity. • **low**: displays information about signatures with low severity. • **medium**: displays information about signatures with medium severity. • **high**: displays information about signatures with high severity.
state { **disabled** | **enabled** | **retired** }	Indicates the state of a predefined signature.	• **disabled**: The predefined signature is disabled. • **enabled**: The predefined signature is enabled. • **retired**: The predefined signature is deprecated.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
target { **server** | **client** | **both** }	Displays signatures by target.	• **server**: displays information about signatures for detecting intrusions into a server. • **client**: displays information about signatures for detecting intrusions into a client. • **both**: displays information about signatures for detecting intrusions into both a client and a server.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ips-signature pre-defined associated** command displays information about predefined associated signatures and user-defined associated signature.

NOTE

If the IPS signature file is not loaded, predefined signatures are not displayed, the protocol cannot be specified, and the category must be set to **all**. You can upgrade services to load the IPS signature file.

Example

Display all predefined signatures.

```
<Huawei> display ips-signature pre-defined
-------------------------------------------------------------------------------
*                    Pre-defined Signature                    *
*                      (Counts: 5538)                         *
-------------------------------------------------------------------------------
Sig-ID   Protocol   Target  Severity OS       Category        Event Counts
-------------------------------------------------------------------------------
1030     HTTP       server  high     windows  Overflow              0
1040     HTTP       client  high     windows  Overflow              0
1050     TCP        server  high     all      Dos                   0
1060     HTTP       server  high     windows  Overflow              0
1080     TCP        server  high     windows  Overflow              0
1090     UDP        server  high     all      Code-execution        0
1100     MSRPC      server  high     windows  Overflow              0
1102     MSRPC      server  high     windows  Overflow              0
1110     TCP        both    high     all      Code-execution        0
1120     TCP        server  high     all      Overflow              0
1140     IMAP4      server  high     unix-like Code-execution       0
1150     MSRPC      server  high     windows  Overflow              0
1160     MSRPC      server  medium   windows  Dos                   0
1170     MSRPC      server  medium   windows  Dos                   0
1189     TCP        server  medium   windows  Dos                   0
1200     SUNRPC     server  high     unix-like Overflow             0
1220     HTTP       client  high     windows  Overflow              0
```

 Copyright © Huawei Technologies Co., Ltd.

```
1230    SUNRPC    server  high    all      Overflow                0
 ---- More ----
```

Display all user-defined signatures.

```
<Huawei> display ips-signature user-defined
 ------------------------------------------------------------------------------
*                    User-defined Signature                      *
*                        (Counts:   1)                          *
 ------------------------------------------------------------------------------
Sig-ID   Protocol   Target  Severity OS       Category        Event Counts
 ------------------------------------------------------------------------------
1        TCP        both    high     N/A      User-defined            0
```

Table 19-110 Description of the **display ips-signature pre-defined** and **display ips-signature user-defined** command output

Item	Description
Counts	Number of signatures
Sig-ID	Signature ID
Protocol	Protocol of packets matching the signature
Target	Detection target of the signature
Severity	Severity of intrusions matching the signature
OS	Operating system attacked by intrusions matching the signature
Category	Signature category
Event Counts	Match count of a signature **NOTE** The Router does not clear the match count of a modified or a deleted user-defined signature. When you create a user-defined signature with an ID the same as that of a deleted signature, the match count increases on the basis of the match count of the deleted signature. For example, the match count of user-defined signature 12 is 10, and the signature is deleted using the **undo ips signature-id** 12 command. If you use the **ips signature-id** 12 command to create a user-defined signature with the same name 12. The match count of the new user-defined signature 12 is 10. To clear the match count of a user-defined or predefined signature, run the **19.9.2.64 reset ips-signature statistics** command.

Display the signature with ID **16042**.

```
<Huawei> display ips-signature 16042
 ------------------------------------------------------------------------------
  SignatureID                : 16042
  Name                       : VideoLAN VLC ActiveX Control Crafted Parameter Memory
Corruption
  Protocol                   : TCP
  Target                     : client
  Severity                   : medium
  OS                         : all
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Category                       : Overflow
  Action                         : alert
  EventCounts                    : 0
  AttackEvidenceCollectionCounts     : 0(slot 0 cpu 0)
  Reference                      : CVE:CVE-2007-6262
  State                          : enabled
  Description                    : CVE-2007-6262 : A certain ActiveX control in axvlc.dll in VideoLAN VLC 0.8.6
before 0.8.6d
allows remote attackers to execute arbitrary code via crafted arguments to the (1) addTarget, (2)
getVariable, or (3) setVariable fu
nction, resulting from a "bad initialized pointer," aka a "recursive plugin release
vulnerability."
 ----------------------------------------------------------------------------
```

Table 19-111 Description of the **display ips-signature** *ips-signature-id* command output

Item	Description
SignatureID	Signature ID
Name	Signature name
Protocol	Protocol of packets matching the signature
Target	Detection target of the signature
Severity	Severity of intrusions matching the signature
OS	Operating system attacked by the intrusions matching the signature
Category	Signature category
Action	Signature action
Threshold	Threshold for signature association times
Interval	Measurement period
Correlateby	Association mode
EventCounts	Match count of a signature **NOTE** To clear the match count of a signature, run the **19.9.2.64 reset ips-signature statistics** command.
AttackEvidenceCollectionCounts	Number of attack evidence collection sessions

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reference	Reference information of a signature • CVE: indicates the Common Vulnerabilities and Exposures (CVE) ID of a signature. You can query the CVE ID on the **http://cve.mitre.org/** website and obtain detailed information based on the CVE ID. • BID: indicates the Bugtraq ID (BID) of a signature. You can query the BID on the **http://www.securityfocus.com/bid** website and obtain detailed information based on the BID. • CNNVD: indicates the China National Vulnerability Database of Information Security (CNNVD) ID of a signature. You can query the CNNVD ID on the **http://www.cnnvd.org.cn/** website and obtain detailed information based on the CNNVD ID.
State	Signature state
Application	Application to which a signature applies
Description	Description of a signature

19.9.2.28 display ips-signature cve-id

Function

The **display ips-signature cve-id** command displays IPS signatures of a specified CVE ID.

Format

display ips-signature cve-id { *cve-id* | **year** *year* }

Parameters

Parameter	Description	Value
cve-id	Specifies a CVE ID.	The value is a string of 13 to 16 characters.
year *year*	Specifies the release year of the CVE.	The value is an integer ranging from 1999 to 2099.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After *cve-id* is specified, this command displays predefined IPS signatures of the specified CVE ID. After *year* is specified, this command displays predefined IPS signatures of the specified release year of CVEs.

Example

Display IPS predefined signatures of the CVE with the ID being CVE-2014-0498.

```
<Huawei> display ips-signature cve-id CVE-2014-0498
 ------------------------------------------------------------------------------
 *                    Pre-defined Signature                     *
 *                      (Counts:    1)                        *
 ------------------------------------------------------------------------------
 Sig-ID   Protocol    Severity   OS          CVE-ID            VENDOR-ID
 ------------------------------------------------------------------------------
 281920   FILE        high       all         CVE-2014-0498     N/A
```

Display IPS predefined signatures of the CVEs released in 2014.

```
<Huawei> display ips-signature cve-id year 2014
 ------------------------------------------------------------------------------
 *                    Pre-defined Signature                     *
 *                      (Counts:   11)                        *
 ------------------------------------------------------------------------------
 Sig-ID   Protocol    Severity   OS          CVE-ID            VENDOR-ID
 ------------------------------------------------------------------------------
 173880   SSL         high       all         CVE-2014-0160     N/A
 269361   SSL         medium     all         CVE-2014-3566     N/A
 167250   FILE        high       windows     CVE-2014-0301
MS14-013
 174331   HTTP        high       windows     CVE-2014-0315
MS14-019
 257330   HTTP        medium     windows     CVE-2014-2880
N/A
 281920   FILE        high       all         CVE-2014-0498     N/A
 284550   HTTP        medium     all         CVE-2014-6039
N/A
 287990   TCP         high       unix-like   CVE-2014-0659     N/A
 291190   FILE        high       all         CVE-2014-0518     N/A
 291910   HTTP        high       windows     CVE-2014-6344
N/A
 269360   SSL         medium     all         CVE-2014-3566     N/A
```

Table 19-112 Description of the **display ips-signature cve-id** command output

Item	Description
Counts	Number of predefined signatures
Sig-ID	ID of a predefined signature
Protocol	Protocol of a predefined signature

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Severity	Severity of a predefined signature, which can be: • high • medium • low • info
OS	Applicable OS of a predefined signature
CVE-ID	CVE ID
VENDOR-ID	Vendor ID

19.9.2.29 display ips-signature statistics

Function

The **display ips-signature statistics** command displays the top-N IPS signatures that are most frequently matched by protocols.

Format

display ips-signature statistics *top-number*

Parameters

Parameter	Description	Value
top-number	Displays the top-N signatures that are most frequently matched.	The value is an integer ranging from 1 to 100.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view top-N IPS signatures that are most frequently matched by protocols, including the protocol, severity, category, and matching count of each signature.

Example

Display the top 6 signatures that are most frequently matched.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ips-signature statistics 6
IPS statistic topN on slot 0 cpu 0:
------------------------------------------------------------------------------
*                    TOP-N Searched Signature                                 *
*                         (Counts:   6)                                      *
------------------------------------------------------------------------------
TOP-N    Sig-ID   Protocol   Severity       Category            Event Counts
------------------------------------------------------------------------------
1        3        TCP        high           User-defined        25
2        2        TCP        high           User-defined        7
3        4        TCP        high           User-defined        3
4        5        TCP        high           User-defined        3
5        6        TCP        high           User-defined        3
6        7        TCP        high           User-defined        3
```

Table 19-113 Description of the **display ips-signature statistics** command output

Item	Description
Counts	Number of signatures
TOP-N	Ranking of signatures in descending order of match count
Sig-ID	Signature ID
Protocol	Protocol of packets matching the signature
Severity	Severity of intrusions matching the signature
Category	Signature category
Event Counts	Match count of a signature **NOTE** To clear the match count of a signature, run the **reset ips-signature statistics** command.

19.9.2.30 display ips-signature vendor-id

Function

The **display ips-signature vendor-id** command displays IPS signatures of a specified vendor ID.

Format

display ips-signature vendor-id *vendor-id*

Parameters

Parameter	Description	Value
vendor-id	Specifies a vendor ID.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ips-signature vendor-id** command displays IPS signatures of a specified vendor ID.

Example

Display all IPS signatures of the vendor ID MS14-013.

```
<Huawei> display ips-signature vendor-id MS14-013
 ------------------------------------------------------------------------------
*                      Pre-defined Signature                                  *
*                        (Counts:    1)                                       *
 ------------------------------------------------------------------------------
Sig-ID   Protocol     Severity    OS          CVE-ID             VENDOR-ID
 ------------------------------------------------------------------------------
167250   FILE          high       windows     CVE-2014-0301      MS14-013
```

Table 19-114 Description of the **display ips-signature vendor-id** command output

Item	Description
Counts	Number of predefined signatures
Sig-ID	ID of a predefined signature
Protocol	Protocol of a predefined signature (protocol used by a network threat)
Severity	Severity of a predefined signature, which can be: • high • medium • low • info
OS	OS targeted by a network threat
CVE-ID	CVE ID
VENDOR-ID	Vendor ID

19.9.2.31 display profile type ips

 Copyright © Huawei Technologies Co., Ltd.

Function

The **display profile type ips** command displays the configuration of an intrusion prevention profile.

Format

display profile type ips [**name** *name* [**signature-set-name** *signature-set-name* | **exception-signature-id** *exception-signature-id*]]

Parameters

Parameter	Description	Value
name *name*	Displays the information about the specified intrusion prevention profile.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-). The value must be an existing intrusion prevention profile.
signature-set-name *signature-set-name*	Specifies the name of a signature filter.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-). The value must be the name of an existing signature filter.
exception-signature-id *exception-signature-id*	Specifies the ID of an exception signature.	The value is an integer ranging from 1 to 16777215. The value must be the ID of an existing exception signature.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The device has multiple default security profiles for different application scenarios as follows. The default security profiles can be displayed, cloned, or referenced in security policies, but cannot be modified or deleted.

Table 19-115 Default intrusion prevention profiles

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
strict	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	All	Block	The intrusion prevention profile applies to the scenarios in which the device is required to block all matched packets.

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
web_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	DNS, HTTP, FTP	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a web server.
file_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	DNS, SMB, NETBIOS, NFS, SUNRPC, MSRPC, FILE, TELNET	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a file server.

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
dns_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	DNS	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a DNS server.
mail_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	DNS, IMAP4, SMTP, POP3	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a mail server.

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
inside_firewall	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	Except **TELNET** and **TFTP**	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed behind a firewall.
dmz	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	Except **NETBIOS**, **NFS**, **SMB**, **TELNET** and **TFTP**	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a .

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
outside_firewall	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	Except **Scanner**	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a firewall.
ids	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	All	Alert	The intrusion prevention profile applies to the scenarios in which the device is deployed off-line as an IDS.

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
default	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in-line as an IPS.

Example

Display the information about profile template **default**.

```
<Huawei> display profile type ips name default
 IPS Profile Configurations:
 ------------------------------------------------------------------------------
 Name                          : default
 Description                   : This profile applies to the general scenario when the device is deployed in IPS
(inline) mode.
 Referenced                    : 1
 State                         : committed
 AttackEvidenceCollection      : disable
 AssocCheck:                   : enable

 SignatureSet                  : default
   Target                      : both
   Severity                    : low medium high
   OS                          : unix-like windows android ios other
   Protocol                    : all
   Category                    : all
   Action                      : default
   Application                 : all

 Exception:
 ID      Action                              Name
 ------------------------------------------------------------------------------

 DNS Protocol Check:

 HTTP Protocol Check:
 ------------------------------------------------------------------------------
```

Display the information about intrusion prevention profile **profile_ips_1**.

 Copyright © Huawei Technologies Co., Ltd.

Display information about signature filter **sig_set1** in intrusion prevention profile **profile_ips_1**.

```
<Huawei> display profile type ips name profile_ips_1 signature-set-name sig_set1
 IPS Profile Signature Set Configurations:
 ------------------------------------------------------------------

 SignatureSet    : sig_set1
   Target        : both
   Severity      : low medium high information
   OS            : unix-like windows android ios other
   Protocol      : all
   Category      : all
   Action        : alert
   Application   : all
 ------------------------------------------------------------------
```

Display information about exception signature **12380** in intrusion prevention profile **profile_ips_1**.

```
<Huawei> display profile type ips name profile_ips_1 exception-signature-id 12380
 IPS Profile Exception Configurations:
 ------------------------------------------------------------------------------
 ID       Action                                 Name
 ------------------------------------------------------------------------------
 12380    allow                                   HP Intelligent Management Center TFTP Server MODE Remote
Code Execution
 ------------------------------------------------------------------------------
```

19.9.2.32 dns domain check

Function

The **dns domain check** command enables the DNS domain name check function.

The **undo dns domain check** command disables the DNS domain name check function.

Format

dns domain check action { **alert** | **block** }

undo dns domain check

Parameters

Parameter	Description	Value
alert	Permits the packet and generates a log if the DNS domain name contains unexpected characters.	-
block	Blocks the packet and generates a log if the DNS domain name contains unexpected characters.	-

Views

Intrusion prevention profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The DNS domain name check function is disabled by default.

After the DNS domain name check function is enabled, the Router permits or blocks traffic and generates a log if any domain name contains unexpected characters.

Example

In the intrusion prevention profile **profile1**, enable the DNS domain name check function and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns domain check action block
```

19.9.2.33 dns domain length check

Function

The **dns domain length check** command enables the DNS domain name length check function.

The **undo dns domain length check** command disables the DNS domain name length check function.

Format

dns domain length check [**max-length** *max-length*] **action** { **alert** | **block** }

undo dns domain length check

Parameters

Parameter	Description	Value
max-length *max-length*	Specifies the maximum DNS domain name length to be checked.	The value is an integer ranging from 1 to 255. The default value is 64.
alert	Permits the packet and generates a log if the DNS domain name is longer than the maximum length.	-
block	Blocks the packet and generates a log if the DNS domain name is longer than the maximum length.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

The DNS domain name length check function is disabled by default.

After the DNS domain name length check function is enabled, the Router permits or blocks traffic and generates a log if the length of any domain name exceeds the specified maximum length. If no maximum length is specified, the default value 64 is used.

Example

In the intrusion prevention profile **profile1**, enable the DNS domain name length check function, specify the maximum length to 255, and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns domain length check max-length 255 action block
```

19.9.2.34 dns malformed-packet check

Function

The **dns malformed-packet check** command enables malformed DNS packet detection.

The **undo dns malformed-packet check** command disables malformed DNS packet detection.

Format

dns malformed-packet check action { **alert** | **block** }

undo dns malformed-packet check

Parameters

Parameter	Description	Value
alert	When the protocol format of a DNS packet is abnormal, the packet is permitted, and a log is recorded.	-
block	When the protocol format of a DNS packet is abnormal, the packet is blocked, and a log is recorded.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, this function is disabled.

Example

In IPS profile **profile1**, enable malformed DNS packet detection and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns malformed-packet check action block
```

19.9.2.35 dns request-type check

Function

The **dns request-type check** command enables DNS request packet type detection.

The **undo dns request-type check** command disables DNS request packet type detection.

Format

dns request-type check { *start-type* [**to** *end-type*] **action** | **default-action** } { **alert** | **allow** | **block** }

undo dns request-type check { **all** | *start-type* [**to** *end-type*] }

Parameters

Parameter	Description	Value
start-type end-type	Indicates the query type of a DNS packet.	The value is an integer ranging from 0 to 65535. The value of *end-type* must be no smaller than that of *start-type*.
action	Indicates the action.	-
default-action	Indicates the default action.	-
allow	The packet is permitted.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
alert	The packet is permitted, and a log is recorded.	-
block	The packet is blocked, and a log is recorded.	-
all	Indicates all query types.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

To detect all query types, set a default action (**default-action**).

You can also detect a specified query type. When the DNS packet query type is as specified, the corresponding processing action is implemented. The default processing action applies to other query types.

By default, this function is disabled.

Example

In IPS profile **profile1**, enable DNS packet query type detection and set the default action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns request-type check default-action block
```

19.9.2.36 dns session request-times check

Function

The **dns session request-times check** command enables the function of checking the number of DNS session request times.

The **undo dns session request-times check** command disables the function of checking the number of DNS session request times.

Format

dns session request-times check [**max-times** *max-time*] **action** { **alert** | **block** }

undo dns session request-times check

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-times *max-time*	Specifies the maximum number of DNS session request times.	The value is an integer ranging from 1 to 65535. The default value is 20.
alert	Permits the packet and generates a log if the number of DNS session request times is greater than the specified maximum value.	-
block	Blocks the packet and generates a log if the number of DNS session request times is greater than the specified maximum value.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

The function of checking the number of DNS session request times is disabled by default.

After this function is enabled, the Router permits or blocks traffic if the number of DNS session request times is greater than the specified maximum value. If no maximum number of request times is specified, the default value 20 is used.

Example

In the intrusion prevention profile **profile1**, enable the function of checking the number of DNS session request times, specify the maximum number of request times to 50, and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns session request-times check max-times 50 action block
```

19.9.2.37 exception ips-signature-id

Function

The **exception ips-signature-id** command adds an IPS signature as an exception.

The **undo exception** command deletes an IPS signature from signature exception.

 Copyright © Huawei Technologies Co., Ltd.

Format

exception ips-signature-id *ips-signature-id* [**action** { **alert** | **allow** | **block** }]

undo exception { **ips-signature-id** *ips-signature-id* | **all** }

Parameters

Parameter	Description	Value
ips-signature-id	Specifies the ID of an IPS signature.	The value is an integer ranging from 1 to 16777215.
action	Specifies the action.	-
alert	Indicates that the device generates an alarm when a packet matches an exception IPS signature.	-
allow	Indicates that the device permits a packet when a packet matches an exception IPS signature.	The default action for the exception signature is **allow**.
block	Indicates that the device denies a packet when a packet matches an exception IPS signature.	-
all	Indicates all signatures.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

This command configures different actions for certain signatures. The security policy preferentially implements the action for the exception signature.

During the IPS signature database update, if the configured exception signature does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

 Copyright © Huawei Technologies Co., Ltd.

Example

In intrusion prevention profile **profile1**, add the IPS signature with ID 2012 to the exception signature, set the action to **alert**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] exception ips-signature-id 2012 action alert
```

19.9.2.38 http multi-host check

Function

The **http multi-host check** command enables detection of HTTP packets with multiple **Host** fields.

The **undo http multi-host check** command disables detection of HTTP packets with multiple **Host** fields.

Format

http multi-host check action { **alert** | **block** }

undo http multi-host check

Parameters

Parameter	Description	Value
action	Specifies the action.	-
alert	When an HTTP packet contains multiple **Host** fields, the packet is permitted, and a log is recorded.	-
block	When an HTTP packet contains multiple **Host** fields, the packet is blocked, and a log is recorded.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, this function is disabled.

Example

In IPS profile **profile1**, enable detection of HTTP packets with multiple **Host** fields and set the action to **block**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http multi-host check action block
```

19.9.2.39 http ssh-over-http check

Function

The **http ssh-over-http check** command enables detection of HTTP traffic involving SSH traffic.

The **undo http ssh-over-http check** command disables detection of HTTP traffic involving SSH traffic.

Format

http ssh-over-http check action { **alert** | **block** }

undo http ssh-over-http check

Parameters

Parameter	Description	Value
action	Specifies the action.	-
alert	When an HTTP traffic contains the SSH traffic, the packet is permitted, and a log is recorded.	-
block	When an HTTP traffic contains the SSH traffic, the packet is blocked, and a log is recorded.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, this function is disabled.

Example

In IPS profile **profile1**, enable detection of HTTP traffic involving SSH traffic and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http ssh-over-http check action block
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.40 http x-forwarded-for check

Function

The **http x-forwarded-for check** command enables detection of the **X-Forwarded-For** field in HTTP packets.

The **undo http x-forwarded-for check** command disables detection of the **X-Forwarded-For** field in HTTP packets.

Format

http x-forwarded-for check { **any** | **whitelist** } **action** { **alert** | **block** }

undo http x-forwarded-for check

Parameters

Parameter	Description	Value
any	When an HTTP packet contains the **X-Forwarded-For** field, an anomaly is detected.	-
whitelist	Detects whether all proxy IP addresses in the **X-Forwarded-For** field match the whitelist. If no, an anomaly is detected.	-
action	Specifies the action.	-
alert	When the **X-Forwarded-For** field in an HTTP packet is abnormal, the packet is permitted, and a log is recorded.	-
block	When the **X-Forwarded-For** field in an HTTP packet is abnormal, the packet is blocked, and a log is recorded.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

If you have configured the detection of whether all proxy IP addresses in the **X-Forwarded-For** field match a whitelist (**whitelist**), you need also to run the **http x-forwarded-for whitelist** command to configure such a whitelist.

By default, this function is disabled.

Example

In IPS profile **profile1**, enable detection of the **X-Forwarded-For** field in HTTP packets and set the action to **block** if the packets contain such a field.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http x-forwarded-for check any action block
```

19.9.2.41 http x-forwarded-for whitelist

Function

The **http x-forwarded-for whitelist** command configures a whitelist used to detect the **X-Forwarded-For** field.

The **undo http x-forwarded-for whitelist** command deletes an existing whitelist.

Format

http x-forwarded-for whitelist ipv4 *ip-address*

undo http x-forwarded-for whitelist { **all** | **ipv4** *ip-address* }

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Indicates an IP address.	The IP address is in dotted decimal format.
all	Deletes all whitelists.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

To use the **http x-forwarded-for check** command to enable the detection of whether all proxy IP addresses in the **X-Forwarded-For** field match a whitelist, you need also to use the **http x-forwarded-for whitelist** command to configure such a whitelist. If not all proxy IP addresses in the **X-Forwarded-For** field match the whitelist, an anomaly is detected.

You can configure a maximum of 32 IP addresses in a whitelist.

Example

In IPS profile **profile1**, configure a whitelist used to detect the **X-Forwarded-For** field and set the IP address to **10.1.1.1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http x-forwarded-for check whitelist action block
[Huawei-profile-ips-profile1] http x-forwarded-for whitelist ipv4 10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.42 ips associated pre-defined

Function

The **ips associated pre-defined** command sets a check item for a predefined associated signature.

The **undo ips associated pre-defined** command cancels the settings of the check item for a predefined associated signature.

Format

ips associated pre-defined signature-id *signature-id* { **threshold** *threshold-value* | **interval** *interval-value* | **correlateby** { **source** | **destination** | **source-destination** } } *

undo ips associated pre-defined { **signature-id** *signature-id* | **all** }

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies the ID of a predefined associated signature.	The value is an integer ranging from 1025 to 16777215.
threshold *threshold-value*	Specifies the threshold for signature association times.	The value is an integer ranging from 1 to 2000. The default value is 30.
interval *interval-value*	Specifies the measurement period. If the number of times the associated signature is detected exceeds *threshold-value* within this period, the predefined associated signature is matched.	The value is an integer ranging from 1 to 7200. The default value is 60.
correlateby	Indicates the association mode.	The default mode is **source-destination**.
source	Collects statistics on the number of times that the associated signature is matched for the same source IP address.	-
destination	Collects statistics on the number of times that the associated signature is matched for the same destination IP address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-destination	Collects statistics on the number of times that the associated signature is matched for the same source and destination IP addresses.	-
all	Restores the check items of all predefined associated signatures to the default values.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the check items of a predefined associated signature cannot meet requirements, you can run the **ips associated pre-defined** command to modify the check items.

During the IPS signature database update, if the configured predefined associated signature does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

Example

Configure check items for a predefined associated signature.

```
<Huawei> system-view
[Huawei] ips associated pre-defined signature-id 16042 threshold 20 interval 30 correlateby source-destination
```

19.9.2.43 ips collect-attack-evidence max-session-number

Function

The **ips collect-attack-evidence max-session-number** command sets the maximum number of attack evidence collection sessions for each IPS signature on each CPU.

The **undo ips collect-attack-evidence max-session-number** command restores the default maximum number of attack evidence collection sessions for each IPS signature on each CPU.

 Copyright © Huawei Technologies Co., Ltd.

Format

ips collect-attack-evidence max-session-number *session-number* [**signature-id** *signature-id*]

undo ips collect-attack-evidence max-session-number [**signature-id** *signature-id*]

Parameters

Parameter	Description	Value
session-number	Specifies the maximum number of attack evidence collection sessions.	The value is an integer ranging from 0 to 50. The default value is 5.
signature-id *signature-id*	Specifies the ID of an IPS signature.	The value is an integer ranging from 1025 to 16777215.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **collect-attack-evidence enable** command is executed, the device starts to collect the attack evidence that match the intrusion prevention profile. You can set the maximum number of sessions in which the device collects attack evidence that match the intrusion prevention profile for each IPS signature on each CPU to collect necessary information for packet tracing, with the impact on system performance controlled to the minimum extent. When the device provides multiple CPUs, the maximum number of attack evidence collection sessions for each IPS signature is the value of *session-number* multiplying the number of CPUs.

The device collects all packets in a matched session. This command specifies the maximum number of matched sessions, not the number of matched packets.

During the IPS signature database update, if the predefined signature for which the maximum number of attack evidence collection sessions is set does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

Example

Set the maximum number of attack evidence collection sessions for the signature **54330** to 10.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ips collect-attack-evidence max-session-number 10 signature-id 54330
```

19.9.2.44 http x-online-host blacklist

Function

The **http x-online-host blacklist** command configures a blacklist used to detect the **X-Online-Host** field.

The **undo http x-online-host blacklist** command deletes an existing blacklist.

Format

http x-online-host blacklist *blacklist*

undo http x-online-host blacklist { **all** | *blacklist* }

Parameters

Parameter	Description	Value
blacklist	Specifies a domain name or IP address.	The value is a string of 4 to 127 characters.
all	Deletes all blacklists.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

To use the **http x-online-host check** command to enable the detection of whether the domain name or IP address in the **X-Online-Host** field matches a blacklist, you need also to use the **http x-online-host blacklist** command to configure such a blacklist. If a domain name or IP address in the **X-Online-Host** field matches the blacklist, an anomaly is detected.

You can configure a maximum of 32 domain names or IP addresses in a blacklist.

Example

In IPS profile **profile1**, configure a blacklist used to detect the **X-Online-Host** field and set the domain name to **www.example.com**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http x-online-host check blacklist action block
[Huawei-profile-ips-profile1] http x-online-host blacklist www.example.com
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.45 http x-online-host check

Function

The **http x-online-host check** command enables detection of the **X-Online-Host** field in HTTP packets.

The **undo http x-online-host check** command disables detection of the **X-Online-Host** field in HTTP packets.

Format

http x-online-host check { **any** | **blacklist** | **multiple** } **action** { **alert** | **block** }

undo http x-online-host check

Parameters

Parameter	Description	Value
any	When an HTTP packet contains the **X-Online-Host** field, an anomaly is detected.	-
blacklist	Detects whether the domain name or IP address in an **X-Online-Host** field matches the blacklist. If yes, an anomaly is detected.	-
multiple	When an HTTP packet contains two or more **X-Online-Host** fields, an anomaly is detected.	-
action	Specifies the action.	-
alert	When the **X-Online-Host** field in an HTTP packet is abnormal, the packet is permitted, and a log is recorded.	-
block	When the **X-Online-Host** field in an HTTP packet is abnormal, the packet is blocked, and a log is recorded.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

If you have configured the detection of whether the domain name or IP address in the **X-Online-Host** field matches a blacklist (**blacklist**), you need also to run the **http x-online-host blacklist** command to configure such a blacklist.

By default, this function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Example

In IPS profile **profile1**, enable detection of the **X-Online-Host** field in HTTP packets and set the action to **block** if the packets contain such a field.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http x-online-host check any action block
```

19.9.2.46 ips log based-on-session

Function

The **ips log based-on-session** command configures IPS threat logs to record source and destination IP addresses by session.

The **undo ips log based-on-session** command configures IPS threat logs to record source and destination IP addresses by packet.

Format

ips log based-on-session

undo ips log based-on-session

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, IPS threat logs record source and destination IP addresses by packets. The source and destination IP addresses in IPS threat logs are the source and destination IP addresses of packets.

After you run the **ips log based-on-session** command to configure IPS threat logs to record source and destination IP addresses by session, the source and destination IP addresses in IPS threat logs are the source and destination IP addresses of the sessions with threat packets.

Example

Configure IPS threat logs to record source and destination IP addresses by session.

```
<Huawei> system-view
[Huawei] ips log based-on-session
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.47 ips log merge enable

Function

The **ips log merge enable** command enables the IPS log aggregation function.

The **undo ips log merge enable** command disables the IPS log aggregation function.

Format

ips log merge enable

undo ips log merge enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the system enables the IPS log aggregation function.

After the log aggregation function is enabled, the IPS aggregates multiple identical IPS logs into one log.

Example

Disable the IPS log aggregation function.

```
<Huawei> system-view
[Huawei] undo ips log merge enable
```

19.9.2.48 ips signature-id

Function

The **ips signature-id** command creates a user-defined signature with the specified ID.

The **undo ips signature-id** command deletes all user-defined signatures or the user-defined signature with the specified ID.

Format

ips signature-id *signature-id*

 Copyright © Huawei Technologies Co., Ltd.

undo ips signature-id { *signature-id* | **all** }

Parameters

Parameter	Description	Value
signature-id	Specifies the ID of a user-defined signature.	The value is an integer ranging from 1 to 1024.
all	Deletes all IPS signatures.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A view is created when you create a user-defined signature. All fields in the signature use the default values.

Example

Create user-defined signature **1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1]
```

19.9.2.49 ips signature-state

Function

The **ips signature-state** command configures the state of predefined signatures.

The **undo ips signature-state** command restores the state of all predefined signatures to their state in the IPS signature database.

Format

ips signature-state [**signature-id** *signature-id*] { **enabled** | **disabled** }

undo ips signature-state

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies the ID of a predefined signature.	The value is an integer ranging from 1025 to 16777215.
enabled	Enables the specified predefined signature.	-
disabled	Disables the specified predefined signature.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can increase threat detection ratio by enabling certain signatures or increase threat detection performance and decrease resource consumption by disabling certain signatures.

After the state of a predefined signature is changed, run **engine configuration commit** to commit the change to apply it.

The **ips signature-state** [**signature-id** *signature-id*] { **enabled** | **disabled** } command is used to enable or disable the specified signature.

If no signature ID is specified, the **ips signature-state** { **enabled** | **disabled** } command is used to enable or disable all predefined signatures.

After the state of a predefined signature is changed and committed, run **display ips signature-state** to check whether the state change takes effect.

During the IPS signature database update, if the predefined signature that has a configured state does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

Example

Enable all predefined signatures, disable predefined signature 12345, and then commit the changes. After that, disable predefined signature 54330 without committing the change. Then, view the state of all predefined signatures.

```
<Huawei> system-view
[Huawei] ips signature-state enabled
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] ips signature-state signature-id 12345 disabled
[Huawei] engine configuration commit
[Huawei] ips signature-state signature-id 54330 disabled
[Huawei] display ips signature-state
------------------------------------------------------------------------
Global    : enabled
Count     : 2
Committed : not committed
------------------------------------------------------------------------
Signature-ID    Configured-State    Default-State    Committed
------------------------------------------------------------------------
54330           disabled            enabled          not committed
12345           disabled            enabled          committed
```

Table 19-116 Description of the **display ips signature-state** command output

Item	Description
Global	Default state for all predefined signatures can be either of the following: • **enabled**: Predefined signatures are enabled by default. • **disabled**: Predefined signatures are disabled by default. • **non-configured**: The default state of predefined signatures is not configured. To set the default state for all predefined signatures, run **ips signature-state** { **enabled** | **disabled** }. If the default state is not specified, the state will be **non-configured**.
Count	Number of predefined signatures with changed state
Committed	Whether all state changes are committed: • **committed**: All state changes are committed. • **not committed**: Not all state changes are committed.
Signature-ID	ID of a predefined signature.
Configured-State	New state of a predefined signature: • **enabled**: A predefined signature is enabled. • **disabled**: A predefined signature is disabled. To change the state of a predefined signature, run **ips signature-state signature-id** *signature-id* { **enabled** | **disabled** }.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default-State	State of predefined signatures in the IPS signature database: ● **enabled**: A predefined signature is enabled. ● **disabled**: A predefined signature is disabled. ● **retired**: A predefined signature is deprecated. A predefined signature marked with retired is deprecated and retained only for checking the history of signatures.
Committed	Whether the state change of a predefined signature is committed: ● **committed**: The state change is committed. ● **not committed**: The state change is not committed.

19.9.2.50 name (user-defined IPS signature view)

Function

The **name** command sets the name of a user-defined signature.

The **undo name** command deletes the name of a user-defined signature.

Format

name *name*

undo name

Parameters

Parameter	Description	Value
name	Specifies the name of a user-defined signature.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 96 characters. If the name contains spaces, the length is 3 to 98 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ('), or hyphens (-).

Views

User-defined IPS signature view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure user-defined signature **1** and name it **mysignature**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
```

19.9.2.51 os (IPS signature filter view)

Function

The **os** command adds the IPS signature of the specified operating system to an IPS signature filter.

The **undo os** command deletes the specified operating system from the condition.

Format

os { **android** | **ios** | **unix-like** | **windows** | **other** } *

undo os [**android** | **ios** | **unix-like** | **windows** | **other**]

Parameters

Parameter	Description	Value
android	Indicates the Android operating system.	-
ios	Indicates the iOS operating system.	-
unix-like	Indicates the UNIX operating system, including Linux, HP_unix, AIX, and Sun operating systems.	-
windows	Indicates the Windows operating system.	-
other	Indicates other operating system.	-

Views

IPS signature filter view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

No default operating system is specified in the IPS signature filter.

You can configure this command if the detected attack targets at an operating system.

other indicates the operating systems other than **android**, **ios**, **unix-like**, and **windows**. Therefore, running the **os** command with parameters **android**, **ios**, **unix-like**, **windows**, and **other** being specified is the same as the default setting.

A user-defined signature applies to all operating systems by default. The applicable operating systems cannot be manually configured.

Example

Configure operating system **unix** in IPS signature filter **hello** in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] os unix-like
```

19.9.2.52 profile type ips copy

Function

The **profile type ips copy** command clones an existing intrusion prevention profile and displays the view of the new profile.

Format

profile type ips copy *old-name* [*new-name*]

Parameters

Parameter	Description	Value
old-name	Specifies the name of an intrusion prevention profile to be cloned.	The value must be the name of an existing intrusion prevention profile.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
new-name	Specifies the name of the new intrusion prevention profile.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you need to create an intrusion prevention profile that is similar to an existing one, clone the existing one or use an intrusion prevention profile template.

If *new-name* is not specified, the default name of the new intrusion prevention profile is *old-name*_n. **n** indicates the number of times the profile has been cloned. It is an integer starting from 1.

Example

Create two intrusion prevention profiles by using profile template **default**.

```
<Huawei> system-view
[Huawei] profile type ips copy default
[Huawei-profile-ips-default_1] quit
[Huawei] profile type ips copy default p_ips_1
[Huawei-profile-ips-p_ips_1]
```

19.9.2.53 profile type ips name

Function

The **profile type ips name** command creates an intrusion prevention profile and displays the profile view.

The **undo profile type ips** command deletes all or the specified intrusion prevention profiles.

Format

profile type ips name *name*

undo profile type ips { **all** | **name** *name* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name	Specifies the name of an intrusion prevention profile.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-).
all	Deletes all intrusion prevention profiles.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

As a security mechanism, intrusion prevention detects intrusions by analyzing network traffic and responds to intrusions accordingly to terminate the intrusion behaviors.

After you create an intrusion prevention profile, run the **19.9.2.70 signature-set name** command in the intrusion prevention profile view to configure a signature filter and run the **19.9.2.37 exception ips-signature-id** command to configure exception signatures.

Example

Create intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1]
```

19.9.2.54 protocol (IPS signature filter view)

Function

The **protocol** command adds the IPS signature of the specified protocol to an IPS signature filter.

The **undo protocol** command deletes the specified protocol from the filtering condition.

 Copyright © Huawei Technologies Co., Ltd.

Format

protocol { *protocol-name* &<1-10> | **all** }

undo protocol { *protocol-name* &<1-10> | **all** }

Parameters

Parameter	Description	Value
protocol-name &<1-10>	Specifies the protocol name. **&<1-10>** indicates that a command can have 1 to 10 such parameter values.	-
all	Indicates all protocols.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

No default protocol is specified in the IPS signature filter.

You can add signatures of a maximum of 10 protocols to the signature filter at a time. To add signatures of more than 10 protocols, repeat this command.

Example

Configure protocols **HTTP** and **SMTP** in IPS signature filter **hello** as the filtering conditions in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] protocol HTTP SMTP
```

19.9.2.55 protocol (user-defined IPS signature view)

Function

The **protocol** command configures the protocol in a user-defined signature.

The **undo protocol** command deletes the protocol from a user-defined signature.

Format

protocol *protocol-name*

undo protocol

Parameters

Parameter	Description	Value
protocol-name	Specifies the name of a protocol in the user-defined signature.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

A user-defined signature contains only one protocol.

The protocol of a predefined signature describes the type of the protocol used by an attack packet.

Example

Configure a user-defined signature. Set the ID to **1**, name to **mysignature**, and protocol to **UDP**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
[Huawei-ips-signature-1] protocol UDP
```

19.9.2.56 rename (IPS signature filter view)

Function

The **rename** command renames an existing IPS signature filter and displays the new signature filter view.

Format

rename *new-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
new-name	Specifies the new name of an existing IPS signature filter.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ('), or hyphens (-).

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Change the name of signature filter **hello** to **hello_1** in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] rename hello_1
[Huawei-profile-ips-profile1-sigset-hello_1]
```

19.9.2.57 rename (user-defined signature rule view)

Function

The **rename** command renames an existing user-defined signature rule and displays the new rule view.

Format

rename *new-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
new-name	Specifies the new name of an existing user-defined signature rule.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-).

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

None

Example

In the user-defined signature rule view, change the name of rule **hello** to **hello_1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] rename hello_1
[Huawei-ips-signature-1-rule-hello_1]
```

19.9.2.58 rename (intrusion prevention profile view)

Function

The **rename** command renames an intrusion prevention profile and displays the new profile view.

Format

rename *new-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
new-name	Specifies the new name of the intrusion prevention profile.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-).

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Change the name of intrusion prevention profile **profile1** to **profile_ips_1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] rename profile_ips_1
[Huawei-profile-ips-profile_ips_1]
```

19.9.2.59 reset cnc domain-filter statistics

Function

The **reset cnc domain-filter statistics** command clears domain name-based filtering statistics.

Format

reset cnc domain-filter { **domain** | **exception** | **domain-name** *domain-name* } **statistics**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
domain	Indicates the malicious domain name.	-
exception	Indicates the exception domain name.	-
domain-name *domain-name*	Specifies a malicious or exception domain name.	The value is a string of 4 to 255 characters.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

This command is used to clear filtering statistics of a domain name (**domain-name** *domain-name*) or a set of domain names (**domain** or **exception**). Run the **19.9.2.20 display cnc domain-filter statistics** command to display the domain name-based filtering statistics to check whether previous statistics are cleared.

Example

Clear filtering statistics on malicious domain names.

```
<Huawei> reset cnc domain-filter domain statistics
```

Clear filtering statistics on malicious domain name **www.example.com**.

```
<Huawei> reset cnc domain-filter domain-name www.example.com statistics
```

19.9.2.60 reset context-awareness information statistics

Function

The **reset context-awareness information statistics** command clears the identification results of the context awareness function.

Format

reset context-awareness information statistics

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After checking the identification results of context awareness by using the **display context-awareness information statistics** command, you can clear the identification results by using the **reset context-awareness information statistics** command. The identification results cannot be restored after being cleared. Therefore, exercise caution when using the command.

Example

Clear the identification results of content awareness.

```
<Huawei> reset context-awareness information statistics
```

19.9.2.61 reset context-awareness statistics

Function

The **reset context-awareness statistics** command resets traffic statistics of different categories by context awareness.

Format

reset context-awareness statistics

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After checking traffic statistics of different categories by context awareness by using the **display context-awareness statistics** command, you can clear the statistics by using the **reset context-awareness statistics** command. The traffic statistics cannot be restored after being cleared. Therefore, exercise caution when using the command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear traffic statistics of different categories by context awareness.

```
<Huawei> reset context-awareness statistics
```

19.9.2.62 reset decoding statistics

Function

The **reset decoding statistics** command clears decoding statistics.

NOTE

Only the AR160 (except AR169RW-P-M9) supports this command.

Format

reset decoding statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

none

Example

Clear decoding statistics.

```
<Huawei> reset decoding statistics
```

19.9.2.63 reset ips statistic

Function

The **reset ips statistic** command clears IPS statistics.

Format

reset ips statistic

Parameters

None

Views

User view

Level

3: Management level

Usage Guidelines

IPS statistics cannot be restored after being cleared. Confirm your operation before clearing them.

Example

Clear IPS statistics.

```
<Huawei> reset ips statistic
```

19.9.2.64 reset ips-signature statistics

Function

The **reset ips-signature statistics** command clears IPS signature statistics.

Format

reset ips-signature statistics { **signature-id** *signature-id* | **all** } { **event** | **collect-attack-evidence** | **all** }

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies the ID of an IPS signature.	The value is an integer ranging from 1 to 16777215. The value must be the ID of an existing IPS signature.
all	Indicates all IPS signatures.	-
event	Indicates the match count of an IPS signature.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
collect-attack-evidence	Indicates the number of attack evidence collection sessions.	-
all	Indicate all statistics.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

IPS signature statistics cannot be restored after being cleared. Exercise caution when running the reset command.

For those IPS signatures with the maximum number of matched attack evidence collection sessions, you can clear the attack evidence collection session statistics to restart the statistics collection.

Example

Clear all statistics of all signatures.

```
<Huawei> reset ips-signature statistics all all
```

Clear the match count of IPS signature No. **54330**.

```
<Huawei> reset ips-signature statistics signature-id 54330 event
```

Clear the statistics on the matched attack evidence collection sessions of IPS signature No. **54330**.

```
<Huawei> reset ips-signature statistics signature-id 54330 collect-attack-evidence
```

19.9.2.65 rule name (user-defined IPS signature view)

Function

The **rule name** command creates a user-defined signature rule with the specified name.

The **undo rule** command deletes all user-defined signature rules or the specified user-defined signature rule.

Format

rule name *name*

undo rule { **name** *name* | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name	Specifies the name of a user-defined signature rule.	The value is a case-sensitive string. If the name does not contain any spaces, the value contains 1 to 32 characters. If the name contains spaces, the value contains 3 to 34 characters, and you must enclose the name with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ('), or hyphens (-).
all	Indicates all user-defined signature rules.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

You can configure a maximum of four rules for one user-defined signature.

You must configure the protocol before you create a user-defined signature rule.

Example

Create user-defined signature rule **hello** in user-defined signature **1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello]
```

19.9.2.66 scope (user-defined signature rule view)

Function

The **scope** command configures the matching scope of a user-defined signature rule.

The **undo scope** command restores the default configuration.

 Copyright © Huawei Technologies Co., Ltd.

Format

scope { **flow** | **message** | **packet** }

undo scope

Parameters

Parameter	Description	Value
flow	Indicates that the user-defined signature rule matches flows.	-
message	Indicates that the user-defined signature rule matches messages.	-
packet	Indicates that the user-defined signature rule matches packets.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

By default, the matching scope of a user-defined signature rule is **packet**.

If you select **flow**, the device detects data flows. The configuration applies only to sessions of application-layer protocols over TCP.

If you select **message**, the device detects each message.

If you select **packet**, the device detects packets, such as TCP request or reply packets.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the matching scope to **packet**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] scope packet
```

19.9.2.67 severity (IPS signature filter view)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **severity** command adds the IPS signature of the specified severity to an IPS signature filter.

The **undo severity** command deletes the specified severity from the filtering condition.

Format

severity { **high** | **medium** | **low** | **information** } *

undo severity [**high** | **medium** | **low** | **information**]

Parameters

Parameter	Description	Value
high	Configure the IPS signature filter so that only signatures of "high" level are matched.	-
medium	Configure the IPS signature filter so that only signatures of "medium" level are matched.	-
low	Configure the IPS signature filter so that only signatures of "low" level are matched.	-
information	Configure the IPS signature filter so that only signatures of "information" level are matched.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

No default severity is specified in the IPS signature filter.

Example

Configure severities **low** and **high** in IPS signature filter **hello** as the filtering conditions in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] severity low high
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.68 severity (user-defined IPS signature view)

Function

The **severity** command configures the severity of a user-defined signature.

The **undo severity** command cancels the severity of a user-defined signature.

Format

severity { **high** | **medium** | **low** | **information** }

undo severity

Parameters

Parameter	Description	Value
high	Indicates the high severity.	-
medium	Indicates the medium severity.	-
low	Indicates the low severity.	-
information	Indicates the information severity.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

The default severity of a user-defined signature is **high**.

Threat severity describes the severity of consequences caused by attacks. Higher severity indicates severer consequences caused by attacks against the signature.

Example

Configure user-defined signature **1**, name it **mysignature** and set the severity to **high**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
[Huawei-ips-signature-1] severity high
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.69 signature-set move

Function

The **signature-set move** command configures the priority of an IPS signature filter.

Format

signature-set move *signature-set-name1* { **before** | **after** } *signature-set-name2*

Parameters

Parameter	Description	Value
signature-set-name1	Specifies the signature filter to be moved.	The value must be the name of an existing signature filter.
before	Moves the signature filter to before the specified signature filter.	-
after	Moves the signature filter to after the specified signature filter.	-
signature-set-name2	Specifies the target signature filter. The signature filter to be moved is moved to before or after the target signature filter.	The value must be the name of an existing signature filter.

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

The IPS signature filter displayed in the front has a higher priority than that in the back. You can run the **display this** command in the intrusion prevention profile view to display the priority of an IPS signature filter.

Example

Move signature filter **hello** to after signature filter **world** in intrusion prevention profile **profile1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set move hello after world
```

19.9.2.70 signature-set name

Function

The **signature-set name** command creates an IPS signature filter and displays its view.

The **undo signature-set** command deletes an IPS signature filter.

Format

signature-set name *name*

undo signature-set { **name** *name* | **all** }

Parameters

Parameter	Description	Value
name	Specifies the name of a signature filter.	The value is a case-sensitive string. If the name does not contain any spaces, the value contains 1 to 32 characters. If the name contains spaces, the value contains 3 to 34 characters, and you must enclose the name with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-).
all	Deletes all IPS signature filters.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create IPS signature filter **hello** in intrusion prevention profile **profile1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello]
```

19.9.2.71 source-ip (user-defined signature rule view)

Function

The **source-ip** command specifies the source IP address to be checked by a user-defined signature rule.

The **undo source-ip** command deletes the source IP address to be checked by a user-defined signature rule.

Format

source-ip { [**ipv4**] *start-ipv4-address* [*end-ipv4-address* | *ipv4-mask-length*] | **any** }

undo source-ip

Parameters

Parameter	Description	Value
start-ipv4-address	Specifies the start IPv4 address.	The value is in dotted decimal notation.
end-ipv4-address	Specifies the end IPv4 address.	The value is in dotted decimal notation.
ipv4-mask-length	Specifies the mask length of the IPv4 address.	The value is an integer ranging from 1 to 32.
any	Indicates any IP address.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

All source IP addresses are checked by the user-defined signature rule by default.

The user-defined signature rule can be used to check a single IP address or all address in an IP address range. To use a user-defined signature rule to check an IP

 Copyright © Huawei Technologies Co., Ltd.

address range, you can specify the start and end IP addresses or the mask-length to define the IP address range.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the source IP address to be checked to **10.1.1.1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] source-ip ipv4 10.1.1.1
```

In user-defined signature with the ID of 1, specify user-defined signature rule **hello** and set the source IP address range from **10.2.2.1** to **10.2.2.100** to be checked.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] source-ip ipv4 10.1.1.1 10.1.1.100
```

19.9.2.72 source-port (user-defined signature rule view)

Function

The **source-port** command specifies the source port to be checked by a user-defined signature rule.

The **undo source-port** command deletes the source port to be checked by a user-defined signature rule.

Format

source-port { *start-port end-port* | **any** }

undo source-port

Parameters

Parameter	Description	Value
start-port	Specifies the start port of a port range to be checked by the user-defined signature rule.	The value is an integer ranging from 1 to 65535.
end-port	Specifies the end port of a port range to be checked by the user-defined signature rule.	The value is an integer ranging from 1 to 65535. The value of *end-port* must be no smaller than that of *start-port*.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
any	Indicates that all source ports are checked by the user-defined signature rule.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

All source ports are checked by the user-defined signature rule by default.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the source port range to a range from **80** to **8080**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] source-port 80 8080
```

19.9.2.73 target (IPS signature filter view)

Function

The **target** command adds the IPS signature of the specified target to an IPS signature filter.

The **undo target** command deletes the specified target from the filtering condition.

Format

target { **both** | **client** | **server** }

undo target

Parameters

Parameter	Description	Value
both	Adds signatures that detect packets to both clients and servers to a signature filter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
client	Adds signatures that detect packets to clients to a signature filter.	-
server	Adds signatures detecting packets to servers to a signature filter.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

No default target is specified in the IPS signature filter.

Example

Configure target **server** in IPS signature filter **hello** in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] target server
```

19.9.2.74 target (user-defined IPS signature view)

Function

The **target** command configures the target of a user-defined signature.

The **undo target** command deletes the target of a user-defined signature.

Format

target { **both** | **client** | **server** }

undo target

Parameters

Parameter	Description	Value
both	Detects attack packets to both clients and servers.	-
client	Detects attack packets to clients.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
server	Detects attack packets to servers.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

A user-defined signature detects attack packets to both clients and servers by default.

For example, For TCP/UDP packets, the initiator is the client, whereas the destination of the TCP/UDP packets is the server.

Example

Configure user-defined signature **1** and set the detection target to **server**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] target server
```

19.9.3 URL Filtering Configuration Commands

NOTE

- The following product models support URL filtering function:
  - AR100&AR120&AR150&AR160&AR200&AR3200 series: All models.
  - AR1200 series: AR1220C, AR1220-8GE, AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: all models except AR2201-48FE, AR2202-48FE, and AR2204.

19.9.3.1 add { blacklist | whitelist } (URL filtering profile view)

Function

The **add { blacklist | whitelist }** command adds blacklist and whitelist rules to the URL filtering profile.

The **undo add { blacklist | whitelist }** command removes blacklist and whitelist rules from the URL filtering profile.

Format

add { **blacklist** | **whitelist** } { **url** *url-text* | **host** *host-text* }

undo add { **blacklist** | **whitelist** } { **url** { *url-text* | **all** } | **host** { *host-text* | **all** } | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
blacklist	Indicates a blacklist rule.	-
whitelist	Indicates a whitelist rule.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
url *url-text*	Specifies a URL rule.	• The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. Pre-processing removes **http://** from the entered character string. • If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is **www.example.com/abc/def?"gh**, you need to enter **www.example.com/abc/def?%22gh**. • * indicates wildcard, which appears at the beginning, middle, or end of an URL and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When the URL is configured as ***abc**, all URLs ending with **abc** are matched. – When the URL is configured as ***a*bcd***, all URLs containing **a** and **bcd** in sequence are matched. – When the URL is configured as **bcd***, all URLs starting with **bcd** are matched. • If a URL does not contain any wildcard, the URL must contain at least four consecutive characters, such as **abcd**. If the URL contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. • If the entered URL ends with **.***, there must be at least three common characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. • If the total length of the entered URL is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **.**. Take ***ab.** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **.**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
url all	Indicates all URL rules.	-
host *host-text*	Specifies a domain name rule.	• The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space. • * indicates wildcard, which appears at the beginning, middle, or end of a domain name and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When a domain name is configured as ***abc**, all domain names ending with **abc** are matched. – When a domain name is configured as ***a*bcd***, all domain names containing **a** and **bcd** in sequence are matched. – When a domain name is configured as **bcd***, all domain names starting with **bcd** are matched. • If a domain name does not contain any wildcard, the domain name must contain at least four consecutive characters, such as **abcd**. If the domain name contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. • If the entered domain name ends with **.***, there must be at least three common characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. • If the total length of the entered domain name is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **.**. Take ***ab.** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **.**.
host all	Indicates all domain name rules.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all URL and domain name rules.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

- Blacklist

  Enterprises can define a blacklist to block the access to specified websites, improve work efficiency, and optimize network resource usage.

  If a requested URL matches the blacklist, the Router blocks the access to the requested website.

- Whitelist

  Enterprises can define a whitelist to allow uncontrolled access to URLs on the whitelist.

  If a requested URL matches the whitelist, the Router grants access to the requested website.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Create a URL filtering profile **profile_development**, and add **www.example.com** to the blacklist.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] add blacklist url www.example.com
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.2 add { url | host } (predefined URL category view)

Function

The **add** { **url** | **host** } command adds a URL or domain name rule to a predefined category.

The **undo add** { **url** | **host** } command removes a URL or domain name rule from a predefined category.

 Copyright © Huawei Technologies Co., Ltd.

Format

add { **url** *url-text* &<1-2> | **host** *host-text* &<1-2> }

undo add { **url** { *url-text* &<1-2> | **all** } | **host** { *host-text* &<1-2> | **all** } }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url-text &<1-2>	Specifies a URL rule. **&<1-2>** indicates that each command can configure a maximum of two strings at a time. When the URL contains over 255 characters, you need to enter two strings. The system automatically places the second string behind the first one to form a complete URL for matching. For example, if you configure **add url www.example.com 123**, the system stores it as **www.example.com123** after processing.	• The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. Pre-processing removes **http://** from the entered character string. • When you enter two strings, the URL obtained by combining the two strings contains a maximum of 480 characters. • If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is **www.example.com/abc/def?"gh**, you need to enter **www.example.com/abc/def?%22gh**. • * indicates wildcard, which appears at the beginning, middle, or end of an URL and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When the URL is configured as ***abc**, all URLs ending with **abc** are matched. – When the URL is configured as ***a*bcd***, all URLs containing **a** and **bcd** in sequence are matched.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		– When the URL is configured as **bcd***, all URLs starting with **bcd** are matched. • If a URL does not contain any wildcard, the URL must contain at least four consecutive characters, such as **abcd**. If the URL contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. • If the entered URL ends with **.***, there must be at least three common characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. • If the total length of the entered URL is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **.**. Take ***ab.** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **.**.
url all	Indicates all URL rules.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
host-text &<1-2>	Specifies a domain name rule. **&<1-2>** indicates that each command can configure a maximum of two strings at a time. When the domain name contains over 255 characters, you need to enter two strings. The system automatically places the second string behind the first one to form a complete domain name for matching. For example, if you configure **add host www.example.com 123**, the system stores it as **www.example.com123** after processing.	• The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space. • When you enter two strings, the domain name obtained by combining the two strings contains a maximum of 480 characters. • * indicates wildcard, which appears at the beginning, middle, or end of a domain name and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When a domain name is configured as ***abc**, all domain names ending with **abc** are matched. – When a domain name is configured as ***a*bcd***, all domain names containing **a** and **bcd** in sequence are matched. – When a domain name is configured as **bcd***, all domain names starting with **bcd** are matched. • If a domain name does not contain any wildcard, the domain name must contain at least four consecutive characters, such as **abcd**. If the domain name contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. • If the entered domain name ends with **.***, there must be at least three common

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. • If the total length of the entered domain name is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **..** Take ***ab.*** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **..**
host all	Indicates all domain name rules.	-

Views

Predefined URL category view

Default Level

2: Configuration level

Usage Guidelines

Before you add a URL rule to a predefined URL category, run the **display url-filter category pre-defined** command to view the *subcategory-id* of the predefined URL category. Then run the **url-filter category pre-defined subcategory-id** *subcategory-id* command to access the predefined URL category view and add the desired URL rule.

Run the **display url-filter category pre-defined subcategory-id** *subcategory-id* command to view existing user-defined URL and domain name rules in the predefined URL category view.

Example

Add a URL rule **www.example.com/news** to the predefined category **General Fashion**, and set the matching mode to **Exact**.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined subcategory-id 200
[Huawei-cate-pre-defined-200] add url www.example.com/news
```

Add a domain name rule **www.example.com** to the predefined category **General Fashion**, and set the matching mode to **Exact**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined subcategory-id 200
[Huawei-cate-pre-defined-200] add host www.example.com
```

Add a URL rule **fashion** to the predefined category **General Fashion**, and set the matching mode to **Keyword**.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined subcategory-id 200
[Huawei-cate-pre-defined-200] add url *fashion*
```

19.9.3.3 add { url | host } (user-defined URL category view)

Function

The **add** { **url** | **host** } command adds a URL or domain name rule to a user-defined category.

The **undo add** { **url** | **host** } command removes a URL or domain name rule from a user-defined category.

Format

add { **url** *url-text* &<1-2> | **host** *host-text* &<1-2> }

undo add { **url** { *url-text* &<1-2> | **all** } | **host** { *host-text* &<1-2> | **all** } }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url-text &<1-2>	Specifies a URL rule. **&<1-2>** indicates that each command can configure a maximum of two strings at a time. When the URL contains over 255 characters, you need to enter two strings. The system automatically places the second string behind the first one to form a complete URL for matching. For example, if you configure **add url www.example.com 123**, the system stores it as **www.example.com123** after processing.	• The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. Pre-processing removes **http://** from the entered character string. • When you enter two strings, the URL obtained by combining the two strings contains a maximum of 480 characters. • If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is **www.example.com/abc/def?"gh**, you need to enter **www.example.com/abc/def?%22gh**. • * indicates wildcard, which appears at the beginning, middle, or end of an URL and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When the URL is configured as ***abc**, all URLs ending with **abc** are matched. – When the URL is configured as ***a*bcd***, all URLs containing **a** and **bcd** in sequence are matched.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		– When the URL is configured as **bcd***, all URLs starting with **bcd** are matched. • If a URL does not contain any wildcard, the URL must contain at least four consecutive characters, such as **abcd**. If the URL contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. • If the entered URL ends with **.***, there must be at least three common characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. • If the total length of the entered URL is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **..** Take ***ab.** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **..**
url all	Indicates all URL rules.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
host-text &<1-2>	Specifies a domain name rule. **&<1-2>** indicates that each command can configure a maximum of two strings at a time. When the domain name contains over 255 characters, you need to enter two strings. The system automatically places the second string behind the first one to form a complete domain name for matching. For example, if you configure **add host www.example.com 123**, the system stores it as **www.example.com123** after processing.	• The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space. • When you enter two strings, the domain name obtained by combining the two strings contains a maximum of 480 characters. • * indicates wildcard, which appears at the beginning, middle, or end of a domain name and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When a domain name is configured as ***abc**, all domain names ending with **abc** are matched. – When a domain name is configured as ***a*bcd***, all domain names containing **a** and **bcd** in sequence are matched. – When a domain name is configured as **bcd***, all domain names starting with **bcd** are matched. • If a domain name does not contain any wildcard, the domain name must contain at least four consecutive characters, such as **abcd**. If the domain name contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. • If the entered domain name ends with **.***, there must be at least three common

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. • If the total length of the entered domain name is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **..** Take ***ab.*** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **..**
host all	Indicates all domain name rules.	-

Views

User-defined URL category view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Add a URL rule **www.example.com** in the view of user-defined URL category **abc** and set the matching mode to **Exact**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name abc
[Huawei-cate-user-defined-abc] add url www.example.com
```

Add a URL rule **bbs** in the view of user-defined **abc** and set the matching mode to **Keyword**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name abc
[Huawei-cate-user-defined-abc] add url *bbs*
```

Add domain name rule **www.example.com** in the view of user-defined category **abc** and set the matching mode to **Exact**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name abc
[Huawei-cate-user-defined-abc] add host www.example.com
```

19.9.3.4 add referer-host

Function

The **add referer-host** command adds referer-host rules to a URL filtering profile.

The **undo add referer-host** command deletes referer-host rules from a URL filtering profile.

Format

add referer-host *host-text*

undo add referer-host { *host-text* | **all** }

Parameters

Parameter	Description	Value
host-text	Specify a host rule.	The value is a string of 4 to 255 characters, without **/**, ****, **#**, **"**, **?**, or spaces.
all	Indicates all host rules.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

If only the whitelist is configured during the access to a specific web page, other links on the specified web page may fail to be accessed. For example: If only the whitelist rule www.example.com is configured during the access to the www.example.com web page, other links that do not use www.example.com as the domain name are inaccessible. To solve the preceding problem, you can run this command to add the referer-host rule to the URL filtering profile. The referer field in an HTTP request will be matched with the referer-host rule. If a match is found, the URL request is allowed. If the referer field in the HTTP request does not match the configured referer-host rule, the user can determine whether to match the referer field with all whitelist rules.

- When the function of matching the referer field in a URL request with whitelist rules is enabled, the referer field will be matched with all whitelist rules. If a match is found, the URL request is allowed.

 Copyright © Huawei Technologies Co., Ltd.

- When the function of matching the referer field with whitelist rules is disabled, the referer field will not be matched with all whitelist rules.

By default, the function of matching the referer field in a URL request with whitelist rules is enabled. If the function is disabled, you can run the **undo referer-filter whitelist-all enable** command to disable it.

The referer field is a part of an HTTP header. A browser adds the referer field to an HTTP request before sending it to a web server, so that the web server can understand the link of the web.

Example

Create URL filtering profile **profile_development**, and add www.example.com to the referer-host rule.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] add referer-host www.example.com
```

19.9.3.5 category action (URL filtering profile view)

Function

The **category action** command specifies the action for a URL category.

The **undo category action** command specifies the default action for a URL category to **allow**.

Format

category { **pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*] } **action** { **allow** | **alert** | **block** }

undo category { **pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*] } **action**

Parameters

Parameter	Description	Value
category-id	Specifies the ID of a predefined URL category.	The value is an integer ranging from 1 to 100.
subcategory-id	Specifies the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.
category-name	Specifies the name of a user-defined URL category.	The URL category has been configured.
allow	Sets the category action to **allow**.	-
block	Sets the category action to **block**.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
alert	Sets the category action to **alert** and records URL filtering logs.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

Run the **display url-filter category pre-defined** command to display the *subcategory-id* of the specified predefined URL category.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the action for the predefined category **P2P** to **block** in the URL filtering profile view.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] category pre-defined subcategory-id 101 action block
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.6 category action mode (URL filtering profile view)

Function

The **category action mode** command configures the action mode of URL filtering.

The **undo category action mode** command restores the default setting.

Format

category action mode { **strict** | **loose** }

undo category action mode

Parameters

Parameter	Description	Value
strict	Indicates the strict mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
loose	Indicates the loose mode.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

The default action mode for URL categories is the strict mode.

If a URL belongs to multiple categories, the Router takes an action based on the action mode.

- Strict: The Router takes the strictest action among all matched categories. For example, a URL belongs to two categories, and the actions are **Alert** and **Block**. In this case, the Router takes the **Block** action.
- Loose: The Router takes the loosest action among all matched categories. For example, a URL belongs to two categories, and the actions are **Alert** and **Block**. In this case, the Router takes the **Alert** action.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the action mode of URL filtering to the loose mode.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] category action mode loose
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.7 category pre-defined control-level (URL filtering profile view)

Function

The **category pre-defined control-level** command sets the control level for predefined URL categories.

The **undo category pre-defined control-level** command sets the default control level for predefined URL categories to user-defined.

Format

category pre-defined control-level { **high** | **low** | **medium** }

undo category pre-defined control-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
high	Sets the control level to **high**.	None
low	Sets the control level to **low**.	It is the default control level.
medium	Sets the control level to **medium**.	None

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

The device performs different actions on different types of websites at different control levels. To view the category control information at a specified level, run the **display url-filter category pre-defined control-level** [**high** | **low** | **medium**] command.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the control level for predefined URL categories to **medium**.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] category pre-defined control-level medium
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.8 default action (URL filtering profile view)

Function

The **default action** command sets the default action for a URL filtering profile.

The **undo default action** command sets the default action for a URL filtering profile to **allow**.

Format

default action { **allow** | **block** | **alert** }

undo default action

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
allow	Sets the default action to **allow**.	-
block	Sets the default action to **block**.	-
alert	Sets the default action to **alert**.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

The default action for a URL filtering profile is **allow**.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the default action for the URL filtering profile **profile_development** to **block** in the URL filtering profile view.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] default action block
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.9 description (URL filtering profile view)

Function

The **description** command configures the description of a URL filtering profile.

The **undo description** command deletes the description of a URL filtering profile.

Format

description *description*

undo description

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
description	Specifies the description of the URL filtering configuration file.	It is a case-sensitive character string of 1 to 128 characters.

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

Descriptive information about a URL filtering profile helps you remember and recognize a URL filtering profile. Run the **display profile type url-filter** command to view the description of the specified URL filtering profile.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the description of the URL filtering profile **abc**.

```
<Huawei> system-view
[Huawei] profile type url-filter name abc
[Huawei-profile-url-filter-abc] description for marketing
[Huawei-profile-url-filter-abc] quit
[Huawei] engine configuration commit
```

19.9.3.10 description (user-defined URL category view)

Function

The **description** command configures the description of a user-defined URL category.

The **undo description** command deletes the description of a user-defined URL category.

Format

description *description*

undo description

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
description	Specifies the description of a user-defined URL category.	It is a case-sensitive character string of 1 to 128 characters.

Views

User-defined URL category view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the description of the user-defined URL category **ud_abc**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name ud_abc
[Huawei-cate-user-defined-ud_abc] description for research
```

19.9.3.11 display profile type url-filter

Function

The **display profile type url-filter** command displays information about URL filtering profiles.

Format

display profile type url-filter

display profile type url-filter name *name* [**blacklist** [**url** *url-text* | **host** *host-text*] | **whitelist** [**url** *url-text* | **host** *host-text*] | **pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*]]

Parameters

Parameter	Description	Value
name *name*	Indicates the name of a URL filtering profile.	The value must be the name of an existing URL filtering profile.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
blacklist	Indicates the URL blacklist of the URL filtering profile.	-
whitelist	Indicates the URL whitelist of the URL filtering profile.	-
url *url-text*	Specifies a URL rule.	-
host *host-text*	Specifies a domain name rule.	-
pre-defined	Indicate the predefined category.	-
category-id *category-id*	Indicates the ID of a predefined URL category.	The value is an integer ranging from 1 to 100.
subcategory-id *subcategory-id*	Indicates the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.
user-defined	Specifies a user-defined category.	-
name *category-name*	Indicates the name of a user-defined URL category.	The URL category must have been configured.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display configuration information about all URL filtering profiles.

```
<Huawei> display profile type url-filter
------------------------------------------------------------------------------
 URL Filtering Profile Configurations:
 Total Profiles: 2
------------------------------------------------------------------------------
 Name        : abc
 Description : -
```

 Copyright © Huawei Technologies Co., Ltd.

```
Referenced  : 0
------------------------------------------------------------------------------
Default Action : Block
------------------------------------------------------------------------------
Action Mode    : Strict
------------------------------------------------------------------------------
Https-Filter   : Disable
------------------------------------------------------------------------------
------------------------------------------------------------------------------
All Whitelist Rule Support Refer: Enable
------------------------------------------------------------------------------
Blacklist Configurations:
------------------------------------------------------------------------------
Type              Blacklist
------------------------------------------------------------------------------
url               www.example.com
host              www.example.com
------------------------------------------------------------------------------
Whitelist Configurations:
------------------------------------------------------------------------------
Type              Whitelist
------------------------------------------------------------------------------
url               www.example.org
host              www.example.org
------------------------------------------------------------------------------
------------------------------------------------------------------------------
RefererList  Configurations:
------------------------------------------------------------------------------
Type              RefererList
------------------------------------------------------------------------------
host              www.example.com
------------------------------------------------------------------------------
URL Pre-defined Category Configurations:
Codes: CID(Category ID), CN(CategoryName), SID(Subcategory ID),
       SN(Subcategory Name)
------------------------------------------------------------------------------
CID CN              SID   SN                                Action
------------------------------------------------------------------------------
1   P2P
                    101   P2P                               Allow
2   Download
                    102   e-Books                           Allow
                    162   Software Download                 Allow
                    163   Picture Download                  Block
                    164   Music/Film Download               Allow
                    165   General Download                  Allow
------------------------------------------------------------------------------
URL User-defined Category Configurations:
------------------------------------------------------------------------------
CID CN              SID   SN                                Action
------------------------------------------------------------------------------
100 User-defined
                    6001  abc                               Allow
                    6002  def                               Block
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Name        : default
Description : -
Referenced  : 0
------------------------------------------------------------------------------
Default Action : Allow
------------------------------------------------------------------------------
Action Mode    : Strict
------------------------------------------------------------------------------
Https-Filter   : Disable
------------------------------------------------------------------------------
------------------------------------------------------------------------------
All Whitelist Rule Support Refer: Enable
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
Blacklist Configurations:
--------------------------------------------------------------------------------
Type             Blacklist
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Whitelist Configurations:
--------------------------------------------------------------------------------
Type             Whitelist
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
RefererList  Configurations:
--------------------------------------------------------------------------------
Type             RefererList
--------------------------------------------------------------------------------
URL Pre-defined Category Configurations:
Codes: CID(Category ID), CN(CategoryName), SID(Subcategory ID),
       SN(Subcategory Name)
--------------------------------------------------------------------------------
CID CN              SID   SN                                  Action
--------------------------------------------------------------------------------
1   P2P
                    101   P2P                                 Allow
2   Download
                    102   e-Books                             Allow
                    162   Software Download                   Allow
                    163   Picture Download                    Allow
                    164   Music/Film Download                 Allow
                    165   General Download                    Allow
--------------------------------------------------------------------------------
URL User-defined Category Configurations:
--------------------------------------------------------------------------------
CID CN              SID   SN                                  Action
--------------------------------------------------------------------------------
100 User-defined
                    6001  abc                                 Block
                    6002  def                                 Block
--------------------------------------------------------------------------------
```

Table 19-117 Description of the **display profile type url-filter** command output

Item	Description
URL Filtering Profile Configurations	Configuration of URL filtering profiles
Total Profiles	Total number of profiles
Name	Name of the URL filtering profile
Description	Description of the URL filtering configuration file
Referenced	Referenced count
Default Action	Default action for the URL filtering profile
Https-Filter	Encrypted-traffic filtering
Blacklist Configurations	Blacklist configuration
Whitelist Configurations	Whitelist configuration
RefererList Configurations	Referer-host configuration
Type	Match type

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Blacklist	URL blacklist
Whitelist	URL whitelist
RefererList	Referer-host
url	URL
host	Domain name

19.9.3.12 display url-filter category

Function

The **display url-filter category** command displays the URL category list.

Format

display url-filter category [**pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id* | **url** *url-text* | **host** *host-text*] | **user-defined** [**name** *category-name* | **url** *url-text* | **host** *host-text*]]

Parameters

Parameter	Description	Value
pre-defined	Displays information on predefined URL categories.	-
category-id	Indicates the ID of a predefined URL category.	The value is an integer ranging from 1 to 100.
subcategory-id	Indicates the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pre-defined url *url-text*	Indicates the URL rule added to a predefined URL category.	The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is www.example.com/abc/def?"gh, you need to enter www.example.com/abc/def?%22gh.
pre-defined host *host-text*	Indicates the domain name rule added to a predefined URL category.	The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space.
user-defined	Displays information on user-defined URL categories.	-
category-name	Indicates the name of a user-defined URL category.	The category must have been configured.
user-defined url *url-text*	Indicates the URL rule added to a user-defined URL category.	The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is www.example.com/abc/def?"gh, you need to enter www.example.com/abc/def?%22gh.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-defined host *host-text*	Indicates the domain name rule added to a user-defined URL category.	The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display url-filter category pre-defined** [**url** *url-text* | **host** *host-text*] command displays only rules added to predefined URL categories but not rules in the predefined URL category database. You can view rules in the predefined URL category database on the web UI. Log in the web UI of the Router, and choose **Object** > **URL Category**. Enter a URL in the search text box and click **Search** to view URL category information.

Example

Display the URL category list.

```
<Huawei> display url-filter category
-------------------------------------------------------------------------------
 URL Pre-defined Category Count: 138
 URL Pre-defined Category List:
 Codes: CID(Category ID), CN(CategoryName), SID(Subcategory ID),
        SN(Subcategory Name)
-------------------------------------------------------------------------------
 CID   CN                    SID   SN
-------------------------------------------------------------------------------
 1     P2P
                           101   P2P
 2     Download
                           102   e-Books
                           162   Software Download
                           163   Picture Download
                           164   Music/Film Download
-------------------------------------------------------------------------------
 URL User-defined Category Count: 1
 URL User-defined Category List:
-------------------------------------------------------------------------------
 CID    CN                  SID      SN
-------------------------------------------------------------------------------
 100    User-defined
                          60001 abc
                          60001 def
-------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-118 Description of the **display url-filter category** command output

Item	Description
URL Pre-defined Category Count	Number of predefined URL categories
URL Pre-defined Category List	List of predefined URL categories
CID	Category ID
CN	Category name
SID	Subcategory ID
SN	Subcategory name
URL User-defined Category Count	Number of user-defined URL categories
URL User-defined Category List	List of user-defined URL categories

Display the predefined category with category ID 2.

```
<Huawei> display url-filter category pre-defined category-id 2
-------------------------------------------------------------------------------
 Category Name        : Download
 Category ID          : 2
 Category Description : Web sites related to download
-------------------------------------------------------------------------------
 Category Configuration Information:
 Codes: SID(Subcategory ID), SN(Subcategory Name)
-------------------------------------------------------------------------------
 SID   SN                                    Type      User-defined URLs/HOSTs
-------------------------------------------------------------------------------

 102   e-Books                                 url       www.example.com.com
                                             host      www.example.com
 162   Software Download                         url       www.example.com.cn
 163   Picture Download
 164   Music/Film Download                       url       www.example.com
 165   General Download
-------------------------------------------------------------------------------
```

Table 19-119 Description of the **display url-filter category pre-defined category-id 2** command output

Item	Description
Category Name	Category name
Category ID	Category ID
Category Description	Category description
Category Configuration Information	Category configuration
SID	Subcategory ID
SN	Subcategory name

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Match type
User-defined URLs/HOSTs	User-defined URL or host

Display the information about predefined subcategory 101.

```
<Huawei> display url-filter category pre-defined subcategory-id 101
-------------------------------------------------------------------------------
  Subcategory Name        : P2P
  Subcategory ID          : 101
  Subcategory Description : Web sites that provide the introduction to and download of P2P
resources, these Web sites are always bound to contain P2P tools such as Thunder and VeryCD,
providing seed download, search, and release
  Category Name           : P2P
  Category ID             : 1
-------------------------------------------------------------------------------
  Subcategory Configuration Information:
-------------------------------------------------------------------------------
                          User-defined URLs/HOSTs
                            (Count: 2)
-------------------------------------------------------------------------------
  Type                 URLs/HOSTs
-------------------------------------------------------------------------------
  url                  www.example.com.com
  host                  www.example.com
-------------------------------------------------------------------------------
```

Table 19-120 Description of the **display url-filter category pre-defined subcategory-id 101** command output

Item	Description
Subcategory Name	Name of a predefined URL subcategory
Subcategory ID	ID of a predefined URL subcategory
Subcategory Description	Description of a user-defined subcategory
Category Name	Name of a predefined URL category
Category ID	ID of a predefined URL category
Subcategory Configuration Information	Subcategory configuration
User-defined URLs/HOSTs	User-defined URL or domain name
Count	Total number user-defined URLs or domain names
Type	Match type

Display the information about the user-defined category **abc**.

```
<Huawei> display url-filter category user-defined name abc
-------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
Category Name          : abc
Category ID            : 60001
Category Description : -
-------------------------------------------------------------------------------
                              User-defined URLs/HOSTs
                                   (Count : 2)
-------------------------------------------------------------------------------
Type                 URLs/HOSTs
-------------------------------------------------------------------------------
url                  www.example.com.com
host                  www.example.com
-------------------------------------------------------------------------------
```

Table 19-121 Description of the **display url-filter category user-defined name abc** command output

Item	Description
Category Name	Name of a user-defined URL category.
Category ID	ID of a user-defined URL category
Category Description	Description of a user-defined URL category
User-defined URLs/HOSTs	User-defined URL or domain name
Count	Total number user-defined URLs or domain names
Type	Match type

Display the rules containing **example.com** in the user-defined category.

```
<Huawei> display url-filter category user-defined host example.com
-------------------------------------------------------------------------------
Matched Count : 2
Matched Result Information:
Codes: SID(Subcategory ID), SN(Subcategory Name)
-------------------------------------------------------------------------------
SID    SN                          Matched URLs/HOSTs
-------------------------------------------------------------------------------
60001  abc                          www.example.com
60002  def                          www.example.com/abc
-------------------------------------------------------------------------------
```

Table 19-122 Description of the **display url-filter category user-defined host example.com** command output

Item	Description
Matched Count	Match count
Matched Result Information	Match result
SID	Subcategory ID
SN	Subcategory name
Matched URLs/HOSTs	Matched URL or domain name

 Copyright © Huawei Technologies Co., Ltd.

19.9.3.13 display url-filter category pre-defined control-level

Function

The **display url-filter category pre-defined control-level** command displays information about all the predefined categories of a specific control level.

Format

display url-filter category pre-defined control-level [**high** | **low** | **medium**]

Parameters

Parameter	Description	Value
high	Displays information about all the predefined categories whose control level is **high**.	-
low	Displays the control level for a predefined category to **low**.	-
medium	Displays the control level for a predefined category to **medium**.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the information about all the predefined categories whose control level is **low**.

```
<Huawei> display url-filter category pre-defined control-level low
------------------------------------------------------------------------------
 Control Level: Low
 URL Pre-defined Category Configurations:
 Codes: CID(Category ID), CN(CategoryName), SID(Subcategory ID)
        SN(Subcategory Name)
------------------------------------------------------------------------------
 CID CN                SID   SN                                  Action
------------------------------------------------------------------------------
 1   P2P
                   101   P2P                                 Allow
 2   Download
                   102   e-Books                             Allow
                   162   Software Download                       Allow
```

```
                163  Picture Download                Allow
                164  Music/Film Download               Allow
                165  General Download                Allow
3  Humanity
                103  History/Culture                 Allow
                166  Literature                      Allow
                167  Arts                            Allow
                168  Music                           Allow
4  Sports
                104  Competitive Sports                Allow
                169  Leisure Sports                  Allow
                170  Sports Equipment                  Allow
.........
```

Table 19-123 Description of the **display url-filter category pre-defined control-level** command output

Item	Description
Control Level	Control level of a predefined category
CID	ID of a predefined URL category.
CN	Name of a predefined URL category
SID	ID of a predefined URL subcategory
SN	Name of a predefined URL subcategory
Action	Available actions: • Allow • Block • Alert

19.9.3.14 display url-filter category statistics

Function

The **display url-filter category statistics** command displays URL category statistics.

Format

display url-filter category { **pre-defined** [**subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*] } **statistics**

Parameters

Parameter	Description	Value
pre-defined	Displays statistics on predefined URL categories.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
subcategory-id *subcategory-id*	Specifies the subcategory ID of a predefined URL category.	The value is an integer ranging from 101 to 60000.
user-defined	Displays statistics on user-defined URL categories.	-
name *category-name*	Specifies the name of a user-defined URL category.	The specified category must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **display url-filter category statistics** command to view the URL category statistics, you can run the **reset url-filter category statistics** command to clear the original statistics and collect statistics again. Cleared statistics cannot be restored. Exercise caution when you run this command.

Example

Display statistics on predefined URL categories.

```
<Huawei> display url-filter category pre-defined statistics
  Statistics Information on slot 11 cpu 0:
------------------------------------------------------------------------------
  Category Statistics Information:
  Codes: SID(Subcategory ID), SN(Subcategory Name), SMN(Subcategory Matched
Num)
------------------------------------------------------------------------------
  SID   SN                                SMN
------------------------------------------------------------------------------
  101   P2P                               0
  102   e-Books                             0
  103   History/Culture                       0
  104   Competitive Sports                      0
  105   Charity/Public Welfare                    0
  106   Military                          0
  108   Blogs/Community                           0
  109   Lottery                           0
  110   Dating/Personals                        0
  111   Cartoon/Animation                         0
  112   Adult Recreational Places                   0
  114   Recreation                          0
  115   Video Games                           0
  117   Toys                              0
  118   Religion                            0
  119   Divining/Supernatural                     0
  122   Adult Suppliers                       0
  123   Gardens/Yards                           0
  ---- More ----
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-124 Description of the **display url-filter category pre-defined statistics** command output

Item	Description
Statistics Information on slot *X* cpu *Y*	Statistics of CPU *Y* in slot *X*
SID	URL subcategory ID
SN	URL subcategory name
SMN	URL subcategory match count

19.9.3.15 display url-filter statistics

Function

The **display url-filter statistics** command displays statistics on URL filtering.

Format

display url-filter statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display URL filtering statistics.

```
<Huawei> display url-filter statistics
------------------------------------------------------------------------------
 Statistics Information:
------------------------------------------------------------------------------
 Total HTTP Requests            : 448460
 Total Permitted HTTP Requests  : 448460
 Total Denied HTTP Requests     : 0
 Matched Blacklist              : 0
 Matched Whitelist              : 0
 Matched User-defined Category  : 0
 Matched Timeout Action         : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Matched Default Action       : 448460
------------------------------------------------------------------------------
```

Table 19-125 Description of the **display url-filter statistics** command output

Item	Description
Statistics Information	Statistics on URL filtering
Total HTTP Requests	Total number of HTTP requests
Total Permitted HTTP Requests	Total number of permitted HTTP requests
Total Denied HTTP Requests	Total number of blocked HTTP requests
Matched Blacklist	Number of times the blacklist is matched
Matched Whitelist	Number of times the whitelist is matched
Matched User-defined Category	Number of times the user-defined category is matched
Matched Timeout Action	Number of times the timeout action is matched
Matched Default Action	Number of times the default action is matched

19.9.3.16 https-filter enable

Function

The **https-filter enable** command enables the encrypted traffic filtering function.

The **undo https-filter enable** command disables the function.

Format

https-filter enable

undo https-filter enable

Parameters

None

Views

URL filtering profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

By default, the function is disabled.

The URL requests sent by users to access desired websites are transmitted using HTTP or HTTPS. For HTTP traffic, the Router can properly implement URL filtering. For HTTPS traffic, the Router can implement URL filtering only after encrypted traffic filtering is configured.

Encrypted traffic filtering takes effect only when it is enabled in the URL filtering profile. If encrypted traffic filtering is disabled in the URL filtering profile, the URL filtering profile does not take effect for HTTPS traffic.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Enable the encrypted traffic filtering function.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_url
[Huawei-profile-url-filter-profile_url] https-filter enable
[Huawei-profile-url-filter-profile_url] quit
[Huawei] engine configuration commit
```

19.9.3.17 import url-sdb file

Function

The **import url-sdb file** command loads the initial URL category database.

Format

import url-sdb file *filename*

Parameters

Parameter	Description	Value
filename	Specifies an initial database file name that contains the absolute path.	The value is a string of 1 to 63 characters without spaces, for example, **hda1:/url.sdb**.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If no initial URL category database is loaded on the device or the initial URL category database needs to be updated, you can manually load the initial URL category database.

If the CF card of the device is damaged, the initial URL category database cannot be loaded. In this case, contact technical support personnel.

Example

Load an initial URL category database.

```
<Huawei> system-view
[Huawei] import url-sdb file hda1:/url.sdb
```

19.9.3.18 profile type url-filter copy

Function

The **profile type url-filter copy** command creates a URL filtering profile (by cloning an existing one) and displays the view of the new URL filtering profile.

Format

profile type url-filter copy *old-name* [*new-name*]

Parameters

Parameter	Description	Value
old-name	Specifies the name of the URL filtering profile to be cloned.	The URL filtering profile must have been configured.
new-name	Specifies the name of the new URL filtering profile.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) are not supported.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can clone an existing URL filtering profile and modify it to create a similar URL filtering profile.

If *new-name* is not specified, the name of the new URL filtering profile is set to "*old-name*_num". **num** indicates the number of times the URL filtering profile is cloned. The value is an integer starting from 1.

Example

Create two URL filtering profiles by cloning the URL filtering profile **abc**.

```
<Huawei> system-view
[Huawei] profile type url-filter copy abc
[Huawei-profile-url-filter-abc_1] quit
[Huawei] profile type url-filter copy abc
[Huawei-profile-url-filter-abc_2] quit
[Huawei]
```

19.9.3.19 profile type url-filter name

Function

The **profile type url-filter name** command creates a URL filtering profile and enters the URL filtering profile view.

The **undo profile type url-filter** command deletes all or specified URL filtering profiles.

Format

profile type url-filter name *name*

undo profile type url-filter { **all** | **name** *name* }

Parameters

Parameter	Description	Value
name	Specifies the name of a URL filtering profile.	The value is a case-sensitive string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.
all	Deletes all URL filtering profiles.	None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you create a URL filtering profile, configure the blacklist, whitelist, user-defined category, and predefined category to specify the URLs that need to be filtered.

Example

Create a URL filtering profile with the name **abc**.

```
<Huawei> system-view
[Huawei] profile type url-filter name abc
[Huawei-profile-url-filter-abc]
```

19.9.3.20 referer-filter whitelist-all enable

Function

The **referer-filter whitelist-all enable** command enables the function for matching the referer field in an HTTP request with all configured whitelist rules.

The **undo referer-filter whitelist-all enable** command disables the function.

Format

referer-filter whitelist-all enable

undo referer-filter whitelist-all enable

Parameters

None

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

By default, the function is enabled. The function can be used to access other links on a specific web page.

 Copyright © Huawei Technologies Co., Ltd.

During URL filtering, if the referer field in an HTTP request sent by a user does not match the referer-host rule configured using the **add referer-host** command, the user can determine whether to match the referer field with all whitelist rules.

- When the function of matching the referer field with whitelist rules is enabled, the referer field will be matched with all whitelist rules. If a match is found, the user can access the website.
- When the function of matching the referer field with whitelist rules is disabled, the referer field will not be matched with all whitelist rules.

Example

Disable the function for matching the referer field in an HTTP request with all configured whitelist rules.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] undo referer-filter whitelist-all enable
```

19.9.3.21 rename (URL filtering profile view)

Function

The **rename** command renames an existing URL filtering profile and displays the new profile view.

Format

rename *new-name*

Parameters

Parameter	Description	Value
new-name	Specifies the new name of the URL filtering profile.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.

Views

URL filtering profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Run the rename command renames an existing URL filtering profile and displays the new profile view.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Rename the URL filtering profile **abc** to **hello**.

```
<Huawei> system-view
[Huawei] profile type url-filter name abc
[Huawei-profile-url-filter-abc] rename hello
[Huawei-profile-url-filter-hello] quit
[Huawei] engine configuration commit
```

19.9.3.22 rename (user-defined URL category view)

Function

The **rename** command renames an existing user-defined URL category and displays the view of the new user-defined URL category.

Format

rename *new-name*

Parameters

Parameter	Description	Value
new-name	Specifies the name of a user-defined URL category.	The value is a string of case-insensitive characters. The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-). • If the value does not contain any space, the value contains 1 to 32 characters. • If the value contains spaces, you must enclose the value with double quotation marks (""), for example, "user for test", and the value contains 3 to 34 characters.

Views

User-defined URL category view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **rename** command to rename a user-defined URL category to facilitate management.

Example

Rename the user-defined URL category **company** to **development**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name company
[Huawei-category-user-defined-company] rename development
[Huawei-category-user-defined-development]
```

19.9.3.23 reset url-filter category statistics

Function

The **reset url-filter category statistics** command clears URL category statistics.

Format

reset url-filter category { **pre-defined** [**subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*] } **statistics**

Parameters

Parameter	Description	Value
pre-defined	Clears statistics on predefined URL categories.	-
subcategory-id *subcategory-id*	Specifies the subcategory ID of a predefined URL category.	The value is an integer ranging from 101 to 60000.
user-defined	Clears statistics on user-defined URL categories.	-
name *category-name*	Specifies the name of a user-defined URL category.	The specified category must already exist.

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After you run the **display url-filter category statistics** command to view the URL category statistics, you can run the **reset url-filter category statistics** command to clear the original statistics and collect statistics again. Cleared statistics cannot be restored. Exercise caution when you run this command.

Example

Clear statistics on predefined URL categories.

```
<Huawei> reset url-filter category pre-defined statistics
```

19.9.3.24 reset url-filter statistics

Function

The **reset url-filter statistics** command clears statistics on URL filtering.

Format

reset url-filter statistics { **blacklist** | **whitelist** | **category** [**user-defined** | **pre-defined**] | **all** }

Parameters

Parameter	Description	Value
blacklist	Indicates the number of times that blacklisted URLs are matched.	-
whitelist	Indicates the number of times whitelisted URLs are matched.	-
user-defined	Indicates the number of times user-defined categories are matched.	-
pre-defined	Indicates the number of times predefined categories are matched.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all URL filtering statistics, including: ● Total number of user-initiated visits, the total number of Router allowed visits, and the total number of Router blocked visits. ● Number of times when whitelisted and blacklisted URLs, and user-defined and pre-defined categories are matched. ● Number of times when the Router performs the timeout action because of query category timeout, and number of times when the Router performs the default action. ● Number of times when abnormal HTTP packets are matched. ● Matching count of a predefined cache entry.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Use caution before you decide to run this command. Once statistics on URL filtering are cleared, they cannot be restored.

Example

Clears all URL filtering statistics.

```
<Huawei> reset url-filter statistics all
```

19.9.3.25 url-filter anti-bypass enable

Function

The **url-filter anti-bypass enable** command enables the abnormal HTTP packet detection function.

The **undo url-filter anti-bypass enable** command disables the abnormal HTTP packet detection function.

Format

url-filter anti-bypass enable

undo url-filter anti-bypass enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the abnormal HTTP packet detection function is disabled.

When the web server has the fault tolerance mechanism or the web server is not designed based on the RFC standard of HTTP, attackers may evade URL filtering. When an attacker tampers with an HTTP packet to make the URL information extracted by the Router different from URL filtering rules, the Router will permit the abnormal HTTP packet. After the abnormal HTTP packet reaches the web server, the server can identify the requested URL. Therefore, the attacker can access the URL.

After you enable the abnormal HTTP packet detection function, the Router can detect abnormal HTTP packets, preventing attackers from evading URL filtering.

Example

Enable abnormal HTTP packet detection.

```
<Huawei> system-view
[Huawei] url-filter anti-bypass enable
```

19.9.3.26 url-filter category pre-defined copy

Function

The **url-filter category pre-defined copy** command clones a predefined URL category.

Format

url-filter category pre-defined copy *subcategory-id new-name*

Parameters

Parameter	Description	Value
subcategory-id	Specifies the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
new-name	Specifies the name of the predefined URL category to be created.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can create a user-defined URL category by cloning an existing predefined URL category and modifying it.

Example

Clone the predefined subcategory 101 and rename the new category as **company**.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined copy 101 company
[Huawei-cate-user-defined-company]
```

19.9.3.27 url-filter category pre-defined subcategory-id

Function

The **url-filter category pre-defined subcategory-id** command displays the predefined subcategory view.

Format

url-filter category pre-defined subcategory-id *subcategory-id*

Parameters

Parameter	Description	Value
subcategory-id	Indicates the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Run the **display url-filter category pre-defined** command to display the *subcategory-id* of the specified predefined URL category.

Example

Display the view of the predefined subcategory **P2P**.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined subcategory-id 101
[Huawei-cate-pre-defined-101]
```

19.9.3.28 url-filter category user-defined copy

Function

The **url-filter category user-defined copy** command clones a user-defined URL category.

Format

url-filter category user-defined copy *old-name* [*new-name*]

Parameters

Parameter	Description	Value
old-name	Indicates the name of a user-defined URL category.	The category must have been configured.
new-name	Indicates the name of the URL category.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

If *new-name* is not specified in the command, the name of the new URL category is the original category name suffixed by **_num**. **_num** indicates the number of times the URL category is cloned.

Example

Clone the user-defined category **company**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined copy company
[Huawei-cate-user-defined-company_1]
```

19.9.3.29 url-filter category user-defined name

Function

The **url-filter category user-defined name** command creates a user-defined URL category and displays the user-defined URL category view.

The **undo url-filter category user-defined** command deletes one or all user-defined URL categories.

Format

url-filter category user-defined name *category-name*

undo url-filter category user-defined { **name** *category-name* | **all** }

Parameters

Parameter	Description	Value
category-name	Specifies the name of a user-defined URL category.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.
all	Indicates all user-defined URL categories.	None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create a user-defined URL category and display the user-defined URL category view.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name abc
```

19.9.3.30 url-filter https-filter consistency-check enable

Function

The **url-filter https-filter consistency-check enable** command enables the encrypted traffic consistency check function.

The **undo url-filter https-filter consistency-check enable** command disables the encrypted traffic consistency check function.

Format

url-filter https-filter consistency-check enable

undo url-filter https-filter consistency-check enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, this function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Usually, URL requests are transmitted through HTTP or HTTPS. The Router can filter HTTP traffic without any additional configuration. To filter HTTPS traffic, the Router must have the encrypted traffic filtering function enabled.

Encrypted traffic filtering of URL filtering does not decrypt HTTPS. Instead, it obtains the domain name (HOST) of the website that a user wants to access by parsing packets.

After the **url-filter https-filter consistency-check enable** command is used to enable encrypted traffic consistency check, the Router extracts the target website domain name (HOST) from the **Server Name Indication** field in the Client Hello packet of the client and the **Common Name** and **Subject Alternative Name** fields in the Certificate packet of the server and verifies the three values during TLS negotiation. In addition, the Router verifies the values of the three fields. The Router implements URL filtering only when the verification succeeds.

The website information contained in the three fields may be tampered with by malicious users. Therefore, some traffic evades URL filtering due to a field verification failure, which affects the detection accuracy of the device.

In whitelist mode (whitelist-only enable), the encrypted traffic consistency check function does not take effect. In whitelist mode, the device allows URL requests only when the ServerName, Common Name, and Subject Alternative Name fields are in the configured whitelist. If the three fields are different, that is, 1.abc.com, 2.abc.com, and 3.abc.com, set the whitelist to *.abc.com.

Example

Enable encrypted traffic consistency check.

```
<Huawei> system-view
[Huawei] url-filter https-filter consistency-check enable
```

19.9.3.31 web-url-filter user-set

Function

The **web-url-filter user-set** command enables user group-based URL filtering.

The **undo web-url-filter user-set** command disables user group-based URL filtering.

By default, user group-based URL filtering is disabled.

Format

web-url-filter user-set *user-set-name* **profile** *profile-name* [**time-range** *time-range-name*] [**description** *description-text*]

undo web-url-filter user-set *user-set-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
user-set-name	Specifies the name of a user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (""), the string can contain spaces.
profile *profile-name*	Specifies the name of a URL filtering profile. **NOTE** A URL filtering profile must be created using the **profile type url-filter name** command and the related parameters must be set.	The value is a string of case-insensitive characters. When the name does not contain spaces, the value is a string of 1 to 32 characters. When the name contains spaces, the value is a string of 3 to 34 characters, and you need to put the string in double quotation marks (""), for example, "user for test". The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-).
time-range *time-range-name*	Indicates the name of the created effective period. **NOTE** The effective period can take effect only after the **time-range** command is executed.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. It cannot contain question marks (?) or spaces. In addition, the word **all** cannot be specified as a time range name.
description *description-text*	Indicates the URL filtering description in the user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (""), the string can contain spaces.

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The web management system supports user group management. You can run the **web-url-filter user-set** command to enable user group-based URL filtering to control the URL addresses the users in the user group can access.

Prerequisites

The **user-set** command has been executed to create a user group.

Example

Enable URL filtering for the user group **huawei**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set huawei
[Huawei-web-user-set-huawei] quit
[Huawei-web] web-url-filter user-set huawei profile abc
```

19.9.3.32 enable web-url-filter user-set

Function

The **enable web-url-filter user-set** command enables user group-based URL filtering.

The **disable web-url-filter user-set** command disables user group-based URL filtering.

By default, user group-based URL filtering is disabled.

Format

enable web-url-filter user-set *user-set-name*

disable web-url-filter user-set *user-set-name* [**profile** *profile-name* [**time-range** *time-range-name*] [**description** *description-text*]]

Parameters

Parameter	Description	Value
user-set-name	Specifies the name of a user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (""), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
profile *profile-name*	Specifies the name of a URL filtering profile. **NOTE** A URL filtering profile must be created using the **profile type url-filter name** command and the related parameters must be set.	The value is a string of case-insensitive characters. When the name does not contain spaces, the value is a string of 1 to 32 characters. When the name contains spaces, the value is a string of 3 to 34 characters, and you need to put the string in double quotation marks (""), for example, "user for test". The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-).
time-range *time-range-name*	Indicates the name of the created effective period. **NOTE** The effective period can take effect only after the **time-range** command is executed.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. It cannot contain question marks (?) or spaces. In addition, the word **all** cannot be specified as a time range name.
description *description-text*	Indicates the URL filtering description in the user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (""), the string can contain spaces.

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The web management system supports user group management. You can run the **enable web-url-filter user-set** command to enable user group-based URL filtering to control the URL addresses the users in the user group can access.

Prerequisites

The **user-set** command has been executed to create a user group.

Example

Enable URL filtering for the user group **huawei**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set huawei
[Huawei-web-user-set-huawei] quit
[Huawei-web] enable web-url-filter user-set huawei
```

19.9.4 Deep Security Maintenance Commands

19.9.4.1 display engine session statistic

Function

The **display engine session statistic** command displays session statistics for the engine.

Format

display engine session statistic

Parameters

None

Views

All views

Level

1: Monitoring level

Usage Guidelines

None

Example

Displays session statistics for the engine.

```
<Huawei> display engine session statistic
 Engine Session Statistic Information of All Threads:
------------------------------------------------------------------------------
   Total Current Sessions                    :         0
   Total Current UDP Sessions                :         0
   Total Current TCP Sessions                :         0
   Total Blocked Sessions                    :         0
   Total Current Free Sessions               :     61440
   Total Current Buffered TCP Segments       :         0
   Total Out-of-sequence TCP Segments        :         0
   Total Overlapping TCP Segments            :         0
   Total Current Free TCP Segments           :      3000
------------------------------------------------------------------------------
Engine Session Statistic Information of Each Thread:
   T00: NgeSess       0, sent:       0 rcv:       0 lost:       0
   T01: NgeSess       0, sent:       0 rcv:       0 lost:       0
   T02: NgeSess       0, sent:       0 rcv:       0 lost:       0
   T03: NgeSess       0, sent:       0 rcv:       0 lost:       0
```

 Copyright © Huawei Technologies Co., Ltd.

```
T04: NgeSess        0, sent:        0 rcv:        0 lost:        0
T05: NgeSess        0, sent:        0 rcv:        0 lost:        0
T06: NgeSess        0, sent:        0 rcv:        0 lost:        0
T07: NgeSess        0, sent:        0 rcv:        0 lost:        0
T08: NgeSess        0, sent:        0 rcv:        0 lost:        0
T09: NgeSess        0, sent:        0 rcv:        0 lost:        0
```

Table 19-126 Description of the **display engine session statistic** command output

Item	Description
Engine Session Statistic Information of All Threads	Session statistics for the engines used by all threads
Total Current Sessions	Total number of all sessions
Total Current UDP Sessions	Total number of UDP sessions
Total Current TCP Sessions	Total number of TCP sessions
Total Blocked Sessions	Total number of blocked sessions
Total Current Free Sessions	Total number of idle session nodes
Total Current Buffered TCP Segments	Total number of cached TCP segments
Total Out-of-sequence TCP Segments	Total number of out-of-sequence TCP segments
Total Overlapping TCP Segments	Total number of overlapped TCP segments
Total Current Free TCP Segments	Total number of TCP segments that can be cached
Engine Session Statistic Information of Each Thread	Session statistics for the engine used by each thread
NgeSess	Number of sessions
sent	Number of sent packets
rcv	Number of received packets
lost	Number of discarded packets

Related Topics

19.9.4.13 reset engine session statistic

19.9.4.2 display engine session table

Function

The **display engine session table** command displays the details about the IPv4 session table of an engine.

 Copyright © Huawei Technologies Co., Ltd.

Format

display engine session table [**source-ip** *source-ip-address* | **source-port** *source-port-number* | **destination-ip** *destination-ip-address* | **destination-port** *destination-port-number* | **protocol** { **tcp** | **udp** }] * [**verbose**]

Parameters

Parameter	Description	Value
source-ip *source-ip-address*	Indicates a source IP address.	-
source-port *source-port-number*	Indicates a source port.	-
destination-ip *destination-ip-address*	Indicates a destination IP address.	-
destination-port *destination-port-number*	Indicates a destination port.	-
protocol	Indicates the protocol field in a session table.	-
tcp	Indicates a TCP session.	-
udp	Indicates a UDP session.	-
verbose	Indicates the details.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display details about the session table of an engine.

```
<Huawei> display engine session table
 VSys:0 Vpn:0 TCP 10.1.1.246:61487-->10.8.1.198:135 ttl:600 left-time:580

 VSys:0 Vpn:0 TCP 10.1.1.197:15141-->10.8.1.227:135 ttl:600 left-time:55

 VSys:0 Vpn:0 UDP 10.6.1.35:35141-->10.8.1.28:111 ttl:120 left-time:19

 VSys:0 Vpn:0 TCP 10.6.1.11:60833-->10.8.1.64:25 ttl:600 left-time:557

 VSys:0 Vpn:0 UDP 10.6.1.192:52189-->10.8.1.245:53 ttl:120 left-time:22

 VSys:0 Vpn:0 TCP 10.6.1.215:47705-->10.8.1.195:135 ttl:600 left-time:290

 ---- More ----
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.4.3 display engine statistic

Function

The **display engine statistic** command displays engine statistics.

Format

display engine statistic

Parameters

None

Views

All views

Level

1: Monitoring level

Usage Guidelines

None

Example

Display engine statistics.

```
<Huawei> display engine statistic
Engine Statistic Table
------------------------------------------------------------------------------
 Total Alert Events  :         0
 Total Block Events  :         0
 ------------------------------------------------------------------------------
  Application              Alert Events              Block Events
 ------------------------------------------------------------------------------
  IPS                             0                         0
  URL-FILTER                      0                         0
------------------------------------------------------------------------------
```

Table 19-127 Description of the **display engine statistic** command output

Item	Description
Engine Statistic Table	The engine statistics table.
Total Alert Events	Total number of all alert sessions.
Total Block Events	Total number of all block sessions.
Application	The application module • IPS • URL-FILTER

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alert Events	Number of alert sessions
Block Events	Number of block sessions

19.9.4.4 display file-frame information

Function

The **display file-frame information** command displays the resources of file frame.

Format

display file-frame information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the resources of file frame.

Table 19-128 Description of the **display file-frame information** command output

Item	Description
Max decompression size	Maximum decompressable file size

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Oversize Acion	Action for the situation that the maximum size of files that can be decompressed is exceeded: • Allow: Allows the file transfer. • Alert: Allows the file transfer and generates a log. • Block: Blocks the file transfer and generates a log.
Max decompression depth	Maximum decompressable layers
Overdepth Acion	Action for the situation that the file decompression depth is exceeded: • Allow: Allows the file transfer. • Alert: Allows the file transfer and generates a log. • Block: Blocks the file transfer and generates a log.
Max compression ratio	Maximum decompression ratio
Breakpoint Resume Protocol	Protocols for which resumable file transfer is disabled: • ALL: HTTP and FTP • HTTP • FTP • None: Resumable file transfer is not enabled.
File frame resources	File frame resource
Decompression handler	Number of handlers used in file decompression, with Total indicating the total number of handlers available in file decompression
File handler cachepool: file handler cache pool	
Thread name	Thread name, which can be: • Work thread: working thread • Total: total number of file handlers
Used	Number of used handlers
Total	Total number of available handlers
Data buffer cachepool: data block cache pool	

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Thread name	Thread name, which can be: • Work thread: working thread • Total: total number of data blocks
Used	Number of used data blocks
Total	Total number of available data blocks

19.9.4.5 display fragment-reassemble configuration

Function

The **display fragment-reassemble configuration** command displays the global fragment reassembly configuration.

Format

display fragment-reassemble configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the global fragment reassembly configuration.

```
<Huawei> display fragment-reassemble configuration
Fragment Reassembly Configuration:
------------------------------------------------------------
enable               : on
overflow-mode        : discard
overlap-mode         : consistency
time-out(s)          : 5
packet-cache(packets) : 255
total-cache(packets)  : 60000
------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-129 Description of the display fragment-reassemble configuration

Item	Description
enable	State of the fragment reassembly function. • on: The function is enabled. • off: The function is disabled.
overflow-mode	Indicates the method for handling packets arriving at a full buffer in fragment reassembly. • discard: Packets arriving at a full buffer are discarded. • forward: Packets arriving at a full buffer are forwarded straight through.
overlap-mode	Indicates the policy to handle overlapping fragments: • consistency: Indicates that overlapping fragments are processed based whether the overlapping parts have the same content.
time-out(s)	Indicates the fragment reassembly timeout in seconds.
packet-cache(packets)	Indicates the fragment buffer size (in number of packets) for each packet.
total-cache(packets)	Indicates the total buffer size in number of packets.

19.9.4.6 display fragment-reassemble session table

Function

The **display fragment-reassemble session table** command displays packet fragment reassembly information in the IAE session table.

Format

display fragment-reassemble session table [**source-ip** *source-ip-address* | **destination-ip** *destination-ip-address*]*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
source-ip *source-ip-address*	Specifies the source IP address.	The value is in dotted decimal notation.
destination-ip *destination-ip-address*	Specifies the destination IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the content security service is configured in the security policy for fragmented packets, the fragmented packets are sent to the IAE for processing. The IAE establishes a session and reassembles the fragmented packets. Using the **display fragment-reassemble session table** command, you can view the packet fragment reassembly information in the IAE session table.

Example

Display IPv4 packet fragment reassembly information in the IAE session table.

```
<Huawei> display fragment-reassemble session table
  VSys:0 Vpn:0 10.1.1.1-->10.2.1.1(363) ttl:5 left-time:4 frag-num:32 flags:(first 1,last 0,overflow 0,result
0)

  VSys:0 Vpn:0 10.1.1.3-->10.2.1.3(363) ttl:5 left-time:3 frag-num:32 flags:(first 1,last 0,overflow 0,result 0)
```

Table 19-130 Description of the **display fragment-reassemble session table** command output

Item	Description
VSys	Name of a virtual system
Vpn	Name of a VPN instance
ttl	Aging time of a fragment session
left-time	Remaining aging time of a fragment session
frag-num	Number of fragments

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
flags:(first 1,last 0,overflow 0,result 0)	Fragment flag, which can be: • first: first fragment • last: last fragment • overflow: fragment cache overflow • result: reassembly result

19.9.4.7 display profile

Function

The **display profile** command displays profile information about all modules.

Format

display profile

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display profile information about all modules.

```
<Huawei> display profile
 Profile Configurations:
 Total Profiles:
 ------------------------------------------------------------------------------
 ProfileName                    ProfileType  Referenced  State
 ------------------------------------------------------------------------------
 strict                       ips          0          committed
 web_server                     ips          0          committed
 file_server                  ips          0          committed
 dns_server                     ips          0          committed
 mail_server                    ips          0          committed
 inside_firewall                ips          0          committed
 dmz                          ips          0          committed
 outside_firewall               ips          0          committed
 ids                          ips          0          committed
```

 Copyright © Huawei Technologies Co., Ltd.

```
default                  ips         1       committed
default                  url-filter  0       committed
```

Table 19-131 Description of the **display profile** command output

Item	Description
Total profiles	Total number of profiles
ProfileName	Name of the profile
ProfileType	Module where the profile belongs to
Referenced	Number of references by a security policy
State	Status of a profile: • committed • not committed

19.9.4.8 display stream-reassemble configuration

Function

The **display stream-reassemble configuration** command displays the global TCP stream reassembly configuration.

Format

display stream-reassemble configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the global TCP stream reassembly configuration.

```
<Huawei> display stream-reassemble configuration
Stream Reassembly Configuration:
```

 Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------
enable               : on
overflow-mode        : forward
overlap-mode         : preserve
session-cache(KB)    : 128
total-cache(packets) : 1024
timestamp-check      : false
tcp-option check     : false
defense-check        : on
session-timeout(s)   : 10
enhanced-mode        : off
-------------------------------------------------------------
```

Table 19-132 Description of the **display stream-reassemble configuration** command output

Item	Description
enable	Indicates the state of the TCP stream reassembly function. ● on: The function is enabled. ● off: The function is disabled.
overflow-mode	Indicates the method for handling packets arriving at a full buffer in stream reassembly. ● discard: Packets arriving at a full buffer are discarded. ● forward: Packets arriving at a full buffer are forwarded straight through.
overlap-mode	Indicates the policy to handle overlapping packets: ● overwrite: Indicate overwrite the original overlapped part. ● preserve: Indicate preserve the original overlapped part.
session-cache(KB)	Indicates the buffer size in KB for each session in TCP stream reassembly.
total-cache(packets)	Global buffer size in number of packets in stream reassembly.
timestamp-check	Indicates the state of the timestamp check function. ● true: The function is enabled. ● false: The function is disabled.
tcp-option check	Indicates the state of the TCP option check function. ● true: The function is enabled. ● false: The function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
defense-check	Indicates the status of the TCP attack defense function: • on: The function is enabled. • off: The function is disabled.
session-timeout(s)	Indicates the timeout of out-of-sequence TCP packet inspection, in seconds.
enhanced-mode	Status of enhanced traffic reassembly: • on: The function is enabled. • off: The function is disabled.

19.9.4.9 fragment-reassemble enable

Function

The **fragment-reassemble enable** command enables fragment reassembly.

The **undo fragment-reassemble enable** command disables fragment reassembly.

Format

fragment-reassemble enable

undo fragment-reassemble enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, fragment reassembly is enabled.

If fragment reassembly is disabled, fragments will not be reassembled and will not be inspected. Meanwhile, TCP stream reassembly may also fail.

Example

Enable fragment reassembly.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] fragment-reassemble enable
```

19.9.4.10 fragment-reassemble overflow-mode

Function

The **fragment-reassemble overflow-mode** command configures the action to take on fragments that overflow the cache.

The **undo fragment-reassemble overflow-mode** command restores the default action to take on fragments that overflow the cache.

By default, the device discards the fragments that overflow the cache.

Format

fragment-reassemble overflow-mode { **discard** | **forward** }

undo fragment-reassemble overflow-mode

Parameters

Parameter	Description	Value
discard	Discards the fragments that overflow the cache.	-
forward	Forwards the fragments that overflow the cache.	-

Views

System view

Level

2: Configuration level

Usage Guidelines

None.

Example

Configure the action to take on fragments that overflow the cache.

```
<Huawei> system-view
[Huawei] fragment-reassemble overflow-mode forward
```

19.9.4.11 fragment-reassemble user-configure

Function

The **fragment-reassemble user-configure** command configures user-defined items for the fragment reassembly function.

 Copyright © Huawei Technologies Co., Ltd.

The **undo fragment-reassemble user-configure** command cancels the configuration of user-defined items for the fragment reassembly function.

Format

fragment-reassemble user-configure { **defense-check** | **pass-through** }

undo fragment-reassemble user-configure { **defense-check** | **pass-through** }

Parameters

Parameter	Description	Value
defense-check	Indicates fragment attack defense.	-
pass-through	Indicates the pass through mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, all user-defined items of the fragment reassembly function are disabled.

After the pass through mode is enabled (using the **fragment-reassemble user-configure pass-through** command), in some special fragment traffic scenarios (for example, the fragments completely overlap, and the overlapped part has the same content), the system will regard the traffic as abnormal traffic and will not reassemble the fragments. If the fragment attack defense function has been enabled (using the **fragment-reassemble user-configure defense-check** command), the abnormal fragments will be discarded. If the fragment attack defense function has not been enabled, the system will forward the fragments. After the pass through mode is disabled, the system assembles the fragments based on the normal processing flow.

Example

Enable the fragment attack defense function.

```
<Huawei> system-view
[Huawei] fragment-reassemble user-configure defense-check
```

19.9.4.12 fragment-reassemble user-configure defense-check

Function

The **fragment-reassemble user-configure defense-check** command enables the fragment attack defense function.

 Copyright © Huawei Technologies Co., Ltd.

The **undo fragment-reassemble user-configure defense-check** command disables the fragment attack defense function.

Format

fragment-reassemble user-configure defense-check

undo fragment-reassemble user-configure defense-check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the fragment attack defense function is disabled.

After this function is enabled, the Router directly discards abnormal fragments.

Example

Enable the fragment attack defense function.

```
<Huawei> system-view
[Huawei] fragment-reassemble user-configure defense-check
```

19.9.4.13 reset engine session statistic

Function

The **reset engine session statistic** command clears the session statistics of the engine.

Format

reset engine session statistic

Parameters

None

Views

User view

Level

3: Management level

Usage Guidelines

NOTE

Use caution before you decide to run this command. Once the session statistics of the engine are cleared, they cannot be restored.

Example

Clear the session statistics of the engine.

```
<Huawei> reset engine session statistic
```

Related Topics

19.9.4.1 display engine session statistic

19.9.4.14 reset engine session table

Function

The **reset engine session table** command clears the session information of the engine.

Format

reset engine session table [**source** *source-ip-address* | **destination** *destination-ip-address* | **destination-port** *destination-port-number* | **protocol** { **tcp** | **udp** }] *

Parameters

Parameter	Description	Value
source *source-ip-address*	Specifies the source IP address.	The value is in dotted decimal notation.
destination *destination-ip-address*	Specifies the destination IP address.	The value is in dotted decimal notation.
destination-port *destination-port-number*	Specifies the destination port number.	The value is an integer ranging from 0 to 65535.
protocol	Indicates a protocol.	-
tcp	Indicates Transmission Control Protocol (TCP).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
udp	Indicates User Datagram Protocol (UDP).	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If no parameter is specified, all session information of the engine is cleared after you run the **reset engine session table** command.

Use caution before you decide to run this command. Clearing the session information of the engine adversely affects the service operating.

Example

Clear all session information of the engine.

```
<Huawei> reset engine session table
Warning: Reseting session table will affect the engine's normal service. Continue? [Y/N]: Y
<Huawei>
```

19.9.4.15 reset engine statistic

Function

The **reset engine statistic** command clears engine statistics.

Format

reset engine statistic

Parameters

None

Views

User view

Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Clear engine statistics.

```
<Huawei> reset engine statistic
```

19.9.4.16 reset fragment-reassemble statistic

Function

The **reset fragment-reassemble statistic** command clears statistics on fragment reassembly.

Format

reset fragment-reassemble statistic

Parameters

None

Views

User view

Level

3: Management level

Usage Guidelines

None

Example

Clear statistics on fragment reassembly.

```
<Huawei> reset fragment-reassemble statistic
```

19.9.4.17 stream-reassemble enable

Function

The **stream-reassemble enable** command enables TCP stream reassembly.

The **undo stream-reassemble enable** command disables TCP stream reassembly.

 Copyright © Huawei Technologies Co., Ltd.

Format

stream-reassemble enable

undo stream-reassemble enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, TCP stream reassembly is enabled.

If TCP stream reassembly is disabled, TCP packets will not be reassembled and will not be inspected. In addition, security inspections based on TCP streams may also fail.

Example

Enable TCP stream reassembly.

```
<Huawei> system-view
[Huawei] stream-reassemble enable
```

19.9.4.18 stream-reassemble enhanced-mode

Function

The **stream-reassemble enhanced-mode** command enables the enhanced traffic reassembly mode.

The **undo stream-reassemble enhanced-mode** command disables the enhanced traffic reassembly mode.

Format

stream-reassemble enhanced-mode

undo stream-reassemble enhanced-mode

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the enhanced traffic reassembly mode is disabled.

The command is used to enable the enhanced traffic reassembly mode in the bypass deployment scenario. After this mode is enabled, sequence number reassembly is supported when TCP data packets and three-way handshake packets are out of order.

Example

Enable the enhanced traffic reassembly mode.

```
<Huawei> system-view
[Huawei] stream-reassemble enhanced-mode
```

19.9.4.19 stream-reassemble overflow-mode

Function

The **stream-reassemble overflow-mode** command configures the action for cache overflow during TCP stream reassembly.

The **undo stream-reassemble overflow-mode** command restores the default action for cache overflow during TCP stream reassembly.

The default action for cache overflow during TCP stream reassembly is **discard**.

Format

stream-reassemble overflow-mode { **discard** | **forward** }

undo stream-reassemble overflow-mode

Parameters

Parameter	Description	Value
discard	Discards the packets that overflow the cache.	-
forward	Forwards the fragments that overflow the cache.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Level

2: Configuration level

Usage Guidelines

None

Example

Set the action for cache overflow during TCP stream reassembly to **forward**.

```
<Huawei> system-view
[Huawei] stream-reassemble overflow-mode forward
```

19.9.4.20 stream-reassemble overlap-mode

Function

The **stream-reassemble overlap-mode** command configures the action for overlapping packets during TCP stream reassembly.

The **undo stream-reassemble overlap-mode** command restores the default action for overlapping packets during TCP stream reassembly.

The default action for the overlapping packets during TCP stream reassembly is **preserve**.

Format

stream-reassemble overlap-mode { **preserve** | **overwrite** }

undo stream-reassemble overlap-mode

Parameters

Parameter	Description	Value
preserve	Preserves overlapping packets.	-
overwrite	Overwrites overlapping packets.	-

Views

System view

Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the action for the overlapping packets during TCP stream reassembly to **overwrite**.

```
<Huawei> system-view
[Huawei] stream-reassemble overlap-mode overwrite
```

19.9.4.21 stream-reassemble session-cache

Function

The **stream-reassemble session-cache** command configures the maximum cache for a session during TCP stream reassembly.

The **undo stream-reassemble session-cache** command restores the maximum cache for a session to the default value during TCP stream reassembly.

By default, the maximum cache for a session during TCP stream reassembly is 32 KB.

Format

stream-reassemble session-cache *session-cache-value*

undo stream-reassemble session-cache

Parameters

Parameter	Description	Value
session-cache-value	Specifies the maximum cache for a session.	The value is an integer ranging from 1 to 32, in KB.

Views

System view

Level

2: Configuration level

Usage Guidelines

None

Example

Set the maximum cache for a session to 16 KB during TCP stream reassembly.

```
<Huawei> system-view
[Huawei] stream-reassemble session-cache 16
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.4.22 stream-reassemble session-timeout

Function

The **stream-reassemble session-timeout** command set the timeout time for out-of-sequence TCP packet inspection.

The **undo stream-reassemble session-timeout** command restores the default setting.

Format

stream-reassemble session-timeout *session-timeout-value*

undo stream-reassemble session-timeout

Parameters

Parameter	Description	Value
session-timeout-value	Specifies the timeout time.	The value is an integer ranging from 0 to 1200, in seconds. The default value is 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, out-of-sequence TCP packet inspection is enabled on the Router.

When *session-timeout-value* is 0, out-of-sequence TCP packet inspection is disabled.

When *session-timeout-value* is greater than 0 and the time when TCP packets are out of order is smaller than or equal to *session-timeout-value*, the Router will attempt to reassemble traffic. If the time when TCP packets are out of order is greater than *session-timeout-value*, the IAE does not detect the content of traffic and ensures traffic transmission preferentially.

Example

Set the timeout time for out-of-sequence TCP packet inspection to 20s.

```
<Huawei> system-view
[Huawei] stream-reassemble session-timeout 20
```

19.9.4.23 stream-reassemble tcp-option check

 Copyright © Huawei Technologies Co., Ltd.

Function

The **stream-reassemble tcp-option check** command enables the TCP option check function.

The **undo stream-reassemble tcp-option check** command disables the TCP option check function.

Format

stream-reassemble tcp-option check

undo stream-reassemble tcp-option check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the TCP option check function is disabled.

After this function is enabled, the engine directly discards packets with abnormal TCP options.

Example

Enable the TCP option check function.

```
<Huawei> system-view
[Huawei] stream-reassemble tcp-option check
```

19.9.4.24 stream-reassemble timestamp check

Function

The **stream-reassemble timestamp check** command enables timestamp check of TCP flow reassembly.

The **undo stream-reassemble timestamp check** command disables timestamp check of TCP flow reassembly.

Format

stream-reassemble timestamp check

undo stream-reassemble timestamp check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you enable timestamp check of TCP flow reassembly, the device verifies the timestamp option of TCP packets. If the option is incorrect, the device discards the packets.

The timestamp check function is disabled by default.

Example

Enable timestamp check of TCP flow reassembly.

```
<Huawei> system-view
[Huawei] stream-reassemble timestamp check
```

19.9.4.25 stream-reassemble user-configure defense-check

Function

The **stream-reassemble user-configure defense-check** command enables the TCP attack defense function.

The **undo stream-reassemble user-configure defense-check** command disables the TCP attack defense function.

Format

stream-reassemble user-configure defense-check

undo stream-reassemble user-configure defense-check

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

By default, the TCP attack defense function is disabled.

After this function is enabled, the Router directly discards abnormal TCP packets.

Example

Enable the TCP attack defense function.

```
<Huawei> system-view
[Huawei] stream-reassemble user-configure defense-check
```

19.10 Local Attack Defense Configuration Commands

19.10.1 application-apperceive

Function

The **application-apperceive** command sets the rate limit for Secure Shell (SSH), Telecommunication Network Protocol (Telnet), Secure Shell Version 6 (SSHv6), Telecommunication Network Protocol Version 6 (Telnetv6), Hypertext Transfer Protocol (HTTP), Border Gateway Protocol (BGP), Internet Key Exchange (IKE), or File Transfer Protocol (FTP) packets after active link protection (ALP) is enabled.

The **undo application-apperceive** command restores the default rate limit for SSH, Telnet, SSHv6, Telnetv6, HTTP, BGP, IKE, or FTP packets.

By default, the rate limit for SSH packets, Telnet packets, SSHv6 packets, Telnetv6 packets, HTTP packets, BGP packets is 512 pps, the rate limit for IKE packets is 128 pps, and the rate limit for FTP packets is 1024 pps.

Format

application-apperceive packet-type { **ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike** } **rate-limit** *rate-value*

undo application-apperceive packet-type { **ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike** }

NOTE

V200R010C10 and later versions support the **ike** parameter.

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
packet-type { **ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike** }	Specifies a packet type. • **ssh**: Indicates that the protocol type is SSH. • **telnet**: Indicates that the protocol type is Telnet. • **sshv6**: Indicates that the protocol type is SSHv6. • **telnetv6**: Indicates that the protocol type is Telnetv6. • **bgp**: Indicates that the protocol type is BGP. • **ftp**: Indicates that the protocol type is FTP. **NOTE** If **ftp** is specified, the rate limit for FTP packets also takes effect for TFTP packets. • **http**: Indicates that the protocol type is HTTP. • **ike**: Indicates that the protocol type is IKE.	-
rate-limit *rate-value*	Specifies the rate limit of protocol packets.	The value is an integer that ranges from 64 to 32768, in pps. When applying the value in pps, the device converts it to a value in kbit/s. The conversion formula is *rate-value* pps = *rate-value* x 1500 x 8/1024 kbit/s.

Views

Attack defense policy view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The default rate limit for application protocol packets such as FTP packets is low. To transmit these packets at a higher rate, run the **application-apperceive** command.

Precautions

If you run the **application-apperceive** command with the same protocol type specified in the same attack defense policy view multiple times, only the latest configuration takes effect.

This command takes effect only when active link protection is enabled by the **19.10.10 cpu-defend application-apperceive enable** command.

Example

Set the rate limit for FTP packets in the attack defense policy **mypolicy** to 1260 pps after ALP is enabled.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] application-apperceive packet-type ftp rate-limit 1260
```

Related Topics

19.10.11 cpu-defend policy

19.10.10 cpu-defend application-apperceive enable

19.10.17 display cpu-defend configuration

19.10.2 auto-defend enable

Function

The **auto-defend enable** command enables automatic attack source tracing.

The **undo auto-defend enable** command disables automatic attack source tracing.

By default, attack source tracing is disabled.

Format

auto-defend enable

undo auto-defend enable

Parameters

None

Views

Attack defense policy view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large number of attack packets may attack the device CPU. Attack source tracing enables the device to trace attack sources and send logs or alarms to notify the administrator so that the administrator can take measures to defend against the attacks. By default, logs are sent to notify the administrator if attack source tracing is enabled.

After automatic attack source tracing is enabled, the device traces the source of the specified packets sent to the CPU. The packet type can be set using the **19.10.6 auto-defend protocol** command.

Precautions

Attack source tracing configured in an attack defense policy takes effect only when the attack defense policy is applied in the system view.

Example

Enable attack source tracing in the attack defense policy named **test**.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
```

Related Topics

19.10.11 cpu-defend policy

19.10.3 auto-defend action

Function

The **auto-defend action** command configures the device to discard packets sent from attack sources.

The **undo auto-defend action** command configures the device not to discard packets sent from attack sources.

By default, the device does not discard packets sent from attack sources.

Format

auto-defend action deny [**timer** *time-length*]

undo auto-defend action

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
deny	Configures the device to discard packets sent from an attack source.	-
timer *time-length*	Specifies the duration in which the device discards packets sent from an attack source.	The value is an integer that ranges from 5 to 86400, in seconds.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The attack source tracing process consists of four phases: packet parsing, traffic analysis, attack source identification, and taking attack source **punish** actions. The **auto-defend action** command is applied to taking attack source **punish** actions. The device discards the packets sent from the identified source.

The **auto-defend action** command configures the device to punish attack sources. When the device detects an attacker, it discards packets sent from the attack source. This protects the device against attacks.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

The device takes **punish** actions on an attack source during the duration specified by **timer** *time-length*. When the duration expires, the device stops discarding packets sent from this attack source. If the attack source continues attacking the device, the device starts to discard packets sent from this attack source again.

Example

Configure the device to discard packets sent from an attack source, and set the duration to 20000 seconds.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] auto-defend enable
[Huawei-cpu-defend-policy-mypolicy] auto-defend action deny timer 20000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.10.11 cpu-defend policy
19.10.2 auto-defend enable

19.10.4 auto-defend alarm enable

Function

The **auto-defend alarm enable** command enables the event reporting function for attack source tracing.

The **undo auto-defend alarm enable** command disables the event reporting function for attack source tracing.

By default, the event reporting function for attack source tracing is disabled.

Format

auto-defend alarm enable

undo auto-defend alarm enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of packets of a specified protocol from an attack source exceeds the threshold in a specified period, the device reports an event to the administrator so that the administrator can take measures to protect the device.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Follow-up Procedure

Run the **auto-defend alarm threshold** command to set the event reporting threshold for attack source tracing.

Example

Enable the event reporting function in the attack defense policy **test**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] auto-defend alarm enable
```

Related Topics

19.10.11 cpu-defend policy

19.10.2 auto-defend enable

19.10.5 auto-defend alarm threshold

19.10.5 auto-defend alarm threshold

Function

The **auto-defend alarm threshold** command sets the event reporting threshold for attack source tracing.

The **undo auto-defend alarm threshold** command restores the default event reporting threshold for attack source tracing.

By default, the event reporting threshold for attack source tracing is 128 pps.

Format

auto-defend alarm threshold *threshold*

undo auto-defend alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the event reporting threshold for attack source tracing.	The value is an integer that ranges from 1 to 65535, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of packets of a specified protocol from an attack source exceeds the threshold in a specified period, the device reports an event to the administrator so that the administrator can take measures to protect the device.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

Attack source tracing has been enabled using the **auto-defend enable** command, and the alarm source tracing function has been enabled using the **auto-defend alarm enable** command.

Precautions

If you run the **auto-defend alarm threshold** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

Example

Set the event reporting threshold for attack source tracing in the attack defense policy named **test** to 300 pps.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] auto-defend alarm enable
[Huawei-cpu-defend-policy-test] auto-defend alarm threshold 300
```

Related Topics

19.10.11 cpu-defend policy

19.10.2 auto-defend enable

19.10.4 auto-defend alarm enable

19.10.6 auto-defend protocol

Function

The **auto-defend protocol** command specifies the types of protocol packets that the device monitors in attack source tracing.

The **undo auto-defend protocol** command deletes specified types of protocol packets that the device monitors in attack source tracing.

By default, the device traces sources of ARP, DHCP, ICMP, IGMP, OSPF, Telnet, TCP, and TTL-expired packets in attack source tracing.

Format

auto-defend protocol { **all** | { **arp** | **dhcp** | **icmp** | **igmp** | **ospf** | **tcp** | **telnet** | **ttl-expired** } * }

undo auto-defend protocol { **arp** | **dhcp** | **icmp** | **igmp** | **ospf** | **tcp** | **telnet** | **ttl-expired** } *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
all	Configures the device to trace sources of ARP, DHCP, ICMP, IGMP, OSPF, Telnet, TCP, and TTL-expired packets in attack source tracing.	-
arp	Adds Address Resolution Protocol (ARP) packets to the list of traced packets or deletes ARP packets from the list.	-
dhcp	Adds Dynamic Host Configuration Protocol (DHCP) packets to the list of traced packets or deletes DHCP packets from the list.	-
icmp	Adds Internet Control Message Protocol (ICMP) packets to the list of traced packets or deletes ICMP packets from the list.	-
igmp	Adds Internet Group Management Protocol (IGMP) packets to the list of traced packets or deletes IGMP packets from the list.	-
ospf	Adds Open Shortest Path First (OSPF) packets to the list of traced packets or deletes OSPF packets from the list.	-
tcp	Adds Transmission Control Protocol (TCP) packets to the list of traced packets or deletes TCP packets from the list.	-
telnet	Adds Telnet packets to the list of traced packets or deletes Telnet packets from the list.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ttl-expired	Adds packets with the TTL value of 1 to the list of traced packets or deletes these packets from the list.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The attack source tracing process consists of four phases: packet parsing, traffic analysis, attack source identification, and taking attack source **punish** actions. The **auto-defend protocol** command is applied to the packet parsing phase. When an attack occurs, you cannot identify the type of attack packets. The **auto-defend protocol** command allows you to flexibly specify the types of traced packets.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend protocol** command multiple times, multiple packet types are specified.

If a packet type is specified, when the device is attacked and the attack source is traced, you can run the **display auto-defend attack-source** command to view attack source information.

Example

Delete IGMP and TTL-expired packets from the list of traced packets.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] undo auto-defend protocol igmp ttl-expired
```

Related Topics

19.10.2 auto-defend enable

19.10.11 cpu-defend policy

19.10.15 display auto-defend attack-source

 Copyright © Huawei Technologies Co., Ltd.

19.10.7 auto-defend threshold

Function

The **auto-defend threshold** command sets the checking threshold for attack source tracing.

The **undo auto-defend threshold** command restores the default checking threshold for attack source tracing.

By default, the checking threshold for attack source tracing is 128 pps.

Format

auto-defend threshold *threshold*

undo auto-defend threshold

Parameters

Parameter	Description	Value
threshold	Specifies the checking threshold for attack source tracing.	The value is an integer that ranges from 1 to 65535, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack source tracing is enabled, you can set the checking threshold for attack source tracing. When the number of sent protocol packets from an attack source in a specified period exceeds the checking threshold, the device traces and logs the attack source.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend threshold** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

After the **auto-defend enable** command is executed, the device traces the attack source based on the default threshold and logs the attack source even if the **auto-defend threshold** command is not used.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the checking threshold for attack source tracing in the attack defense policy named **test** to 200 pps.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] auto-defend threshold 200
```

Related Topics

19.10.11 cpu-defend policy

19.10.2 auto-defend enable

19.10.8 auto-defend trace-type

Function

The **auto-defend trace-type** command configures an attack source tracing mode.

The **undo auto-defend trace-type** command deletes an attack source tracing mode.

By default, attack source tracing is based on source MAC addresses, source IP addresses, and source ports+VLANs.

Format

auto-defend trace-type { **source-mac** | **source-ip** | **source-portvlan** } *

undo auto-defend trace-type { **source-mac** | **source-ip** | **source-portvlan** } *

Parameters

Parameter	Description	Value
source-mac	Configures attack source tracing based on source MAC addresses so that the device classifies and collects statistics based on the source MAC address and identifies the attack source.	-
source-ip	Configures attack source tracing based on source IP addresses so that the device classifies and collects statistics based on the source IP address and identifies the attack source.	-
source-portvlan	Configures attack source tracing based on source ports +VLANs so that the device classifies and collects statistics based on the source port and VLAN and identifies the attack source.	-

Views

Attack defense policy view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling attack source tracing, you can specify one or more attack source tracing modes. The device then uses the specified modes to trace attack sources.

The device supports the following attack source tracing modes:

- Source IP address-based tracing: defends against Layer 3 attack packets.
- Source MAC address-based tracing: defends against Layer 2 attack packets with a fixed source MAC address.
- Source port+VLAN based tracing: defends against Layer 2 attack packets with different source MAC addresses.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend trace-type** command multiple times, multiple attack source tracing modes are specified.

After the attack source tracing function is enabled on the device, you can run the **display auto-defend attack-source** command to view attack source tracing information if an attack occurs.

By default, the device traces attack sources based on source MAC addresses, source IP addresses, and source ports+VLANs. To cancel an attack source tracing mode, run the **undo auto-defend trace-type** command.

Example

Configure attack source tracing based on source MAC addresses.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] undo auto-defend trace-type source-ip source-portvlan
```

Related Topics

19.10.11 cpu-defend policy

19.10.15 display auto-defend attack-source

19.10.9 blacklist

Function

The **blacklist** command configures a blacklist.

The **undo blacklist** command deletes a blacklist.

 Copyright © Huawei Technologies Co., Ltd.

By default, no blacklist is configured.

Format

blacklist *blacklist-id* **acl** *acl-number*

undo blacklist *blacklist-id*

Parameters

Parameter	Description	Value
blacklist-id	Specifies the ID of a blacklist.	The value is an integer that ranges from 1 to 8.
acl *acl-number*	Specifies the number of an Access Control List (ACL) referenced by a blacklist.	The value is an integer that ranges from 2000 to 4999. ● 2000 to 2999: basic ACLs ● 3000 to 3999: advanced ACLs ● 4000 to 4999: Layer 2 ACLs

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To defend against malicious packet attacks, the device uses ACLs to add users with the specific characteristic into a blacklist and discards the packets from the users in the blacklist.

A maximum of 8 blacklists can be configured in an attack defense policy on the device.

Precautions

If multiple blacklists need to be configured in an attack defense policy: Layer 2 ACLs and basic ACLs cannot be used together in these blacklists. Layer 2 ACLs and advanced ACLs cannot be used together in these blacklists. Basic ACLs, advanced ACLs, and Layer 2 ACLs cannot be used together in these blacklists. For example:

- For example, three blacklists are configured in the attack defense policy **mypolicyA**: blacklist1, blacklist2, and blacklist3. If blacklist1 uses a basic ACL,

 Copyright © Huawei Technologies Co., Ltd.

blacklist2 and blacklist3 can use only basic ACLs or advanced ACLs but not Layer 2 ACLs.

- For example, three blacklists are configured in the attack defense policy **mypolicyB**: blacklist1, blacklist2, and blacklist3. If blacklist1 uses a Layer 2 ACL, blacklist2 and blacklist3 can use only Layer 2 ACLs.

Example

Specify ACL 2001 as the rule of blacklist 2.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] blacklist 2 acl 2001
```

Related Topics

19.7.4 acl (system view)

19.10.11 cpu-defend policy

19.10.10 cpu-defend application-apperceive enable

Function

The **cpu-defend application-apperceive enable** command enables active link protection (ALP).

The **undo cpu-defend application-apperceive enable** command disables ALP.

By default, ALP is enabled for SSH, Telnet, SSHv6, Telnetv6, FTP, BGP, IKE, and HTTP.

Format

cpu-defend application-apperceive [**ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike**] **enable**

undo cpu-defend application-apperceive [**ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike**] **enable**

NOTE

V200R010C10 and later versions support the **ike** parameter.

Parameters

Parameter	Description	Value
ssh	Indicates that the protocol type is SSH.	-
telnet	Indicates that the protocol type is Telnet.	-
sshv6	Indicates that the protocol type is SSHv6.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
telnetv6	Indicates that the protocol type is Telnetv6.	-
bgp	Indicates that the protocol type is BGP.	-
ftp	Indicates that the protocol type is FTP. **NOTE** If **ftp** is specified, ALP for FTP packets also takes effect for TFTP packets.	-
http	Indicates that the protocol type is HTTP.	-
ike	Indicates that the protocol type is IKE.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ALP protects session-based application layer data, including data of SSH sessions, Telnet sessions, SSHv6 sessions, Telnetv6 sessions, HTTP sessions, FTP sessions, IKE sessions, and BGP sessions to ensure uninterrupted services when attacks occur.

- When the device communicates with another host or device using FTP, burst traffic of FTP packets occurs. As a result, burst traffic is discarded because it exceeds the rate limit after ALP is enabled on the device or services are interrupted because other FTP packets attack the device.
- When the device attempts to establish a BGP, an HTTP, a SSH, a Telnet, a SSHv6, or a Telnetv6 connection with another host or device, burst traffic of BGP, HTTP, SSH, Telnet, SSHv6, or Telnetv6 packets occurs. As a result, burst traffic is discarded because it exceeds the rate limit after ALP is enabled on the device or a BGP, an HTTP, a SSH, a Telnet, a SSHv6, or a Telnetv6 connection fails to be established because other BGP, HTTP, SSH, Telnet, SSHv6, or Telnetv6 packets attack the device.

When the device detects setup of SSH sessions, Telnet sessions, SSHv6 Session, Telnetv6 Session, HTTP sessions, FTP sessions, IKE sessions, and BGP sessions, ALP is enabled to protect the session. The packets matching characteristics of the session are sent at a high rate; therefore, reliability and stability of session-related services are ensured.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Run the **cpu-defend-policy** command on an LPU to apply the attack defense policy. Then the device protects data flows using the rate limit specified in the active link protection function.

Example

Enable ALP so that the rate limit after ALP is enabled in the attack defense policy **mypolicy** on the main control board takes effect.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] application-apperceive packet-type ftp rate-limit 12600
[Huawei-cpu-defend-policy-mypolicy] quit
[Huawei] cpu-defend application-apperceive enable
[Huawei] cpu-defend-policy mypolicy
```

Related Topics

19.10.11 cpu-defend policy

19.10.17 display cpu-defend configuration

19.10.1 application-apperceive

19.10.11 cpu-defend policy

Function

The **cpu-defend policy** command creates an attack defense policy and displays the attack defense policy view.

The **undo cpu-defend policy** command deletes an attack defense policy.

By default, the **default** attack defense policy exists on the device and is applied to all boards. The **default** attack defense policy cannot be deleted or modified.

Format

cpu-defend policy *policy-name*

undo cpu-defend policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an attack defense policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A large number of packets including malicious attack packets are sent to the CPU on a network. If excess packets are sent to the CPU, the CPU usage becomes high and CPU performance deteriorates. The attack packets affect services and may even cause system breakdown. To solve the problem, create an attack defense policy and configure CPU attack defense and attack source tracing in the attack defense policy.

Precautions

The device supports a maximum of 19 attack defense policies, including the **default** attack defense policy. The **default** attack defense policy is generated in the system by default and is applied to all boards. The **default** attack defense policy cannot be deleted or modified. The other 18 policies can be created, modified, and deleted.

The configuration in a user-defined attack defense policy overrides the configuration in the **default** attack defense policy. If no parameter is set in the user-defined attack defense policy, the configuration in the **default** attack defense policy is used.

Example

Create an attack defense policy named **test**.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test]
```

Related Topics

19.10.18 display cpu-defend policy

19.10.12 cpu-defend-policy

Function

The **cpu-defend-policy** command applies an attack defense policy.

The **undo cpu-defend-policy** command cancels the application of an attack defense policy.

By default, the **default** attack defense policy is applied to all cards.

Format

cpu-defend-policy *policy-name* [**global** | **slot** *slot-id*]

undo cpu-defend-policy [**global** | **slot** *slot-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an attack defense policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.
global	Indicates that the attack defense policy is applied globally. If **global** is specified, the attack defense policy is applied to all interface cards.	-
slot *slot-id*	Indicates that the attack defense policy is applied locally. *slot-id* specifies the slot ID of the LPU. If **slot** is specified, the attack defense policy is applied to specified interface cards. **NOTE** If either **global** or **slot** is specified, the attack defense policy is applied on the main control board.	Set *slot-id* according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An attack defense policy takes effect only when it is applied to a board and only one attack defense policy can be applied to a board.

Prerequisites

An attack defense policy has been created by using the **19.10.11 cpu-defend policy** command.

Precautions

If an attack defense policy has been applied to an LPU in a specified slot, you must run the **undo cpu-defend-policy slot** *slot-id* command to unbind the attack

 Copyright © Huawei Technologies Co., Ltd.

defense policy from the LPU so that you can run the **cpu-defend-policy** *policy-name* **global** command to apply the attack defense policy to all LPUs.

Example

Apply the attack defense policy named **test** to the main control board.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] quit
[Huawei] cpu-defend-policy test
```

Apply the attack defense policy named **test** to all cards.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] quit
[Huawei] cpu-defend-policy test global
```

Related Topics

19.10.11 cpu-defend policy

19.10.13 deny

Function

The **deny** command configures the device to discard packets sent to the CPU.

The **undo deny** command restores the default action taken for the packets sent to the CPU.

By default, the device does not discard packets sent to the CPU. Instead, the device limits the rate of packets sent to the CPU using the default rate. You can check the rate limit of each type of packets using the **display cpu-defend configuration** command.

Format

deny packet-type *packet-type*

undo deny packet-type *packet-type*

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the type of the packet to be discarded.	The supported packet type depends on the device.

Views

Attack defense policy view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After an attack defense policy is created, if the device receives attack packets of a specified type or a large number of packets sent to the CPU, run the **deny** command to configure the device to discard packets of the specified type sent to the CPU.

Precautions

After the **deny** command is executed, the **packet-type** command cannot take effect. After the **undo deny** command is executed, you can run the **packet-type** command to set the rate limit for the packets sent to the CPU.

Example

Configure the drop action taken for ARP Reply packets to be sent to the CPU in the attack defense policy **test**.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] deny packet-type arp-reply
```

Related Topics

19.10.11 cpu-defend policy

19.10.18 display cpu-defend policy

19.10.21 packet-type

19.10.14 description (attack defense policy view)

Function

The **description** command configures the description of an attack defense policy.

The **undo description** command deletes the description of an attack defense policy.

By default, no description is configured for an attack defense policy.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the content of a description.	It is a string of 1 to 63 case-sensitive characters with spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the description of an attack defense policy, for example, the usage or application scenario of the attack defense policy. The description is used to differentiate attack defense policies.

Precautions

If you run the **description** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

Example

Configure the description **defend_arp_attack** for the attack defense policy named **test**.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] description defend_arp_attack
```

Related Topics

19.10.11 cpu-defend policy

19.10.15 display auto-defend attack-source

Function

The **display auto-defend attack-source** command displays the attack sources on the SRU.

Format

display auto-defend attack-source [**detail**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
detail	Displays detailed information about the attack sources on the SRU, including the type of attack packets. If **detail** is not specified, brief information about the attack sources on the SRU is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display auto-defend attack-source** command displays the attack source list.

Example

Display the attack source list on the SRU.

```
<Huawei> display auto-defend attack-source
 Attack Source User Table:
 ------------------------------------------------------------------------------
    MacAddress       InterfaceName      Vlan:Outer/Inner      TOTAL
 ------------------------------------------------------------------------------
 0000-0000-0023       Ethernet2/0/0         199/299            1264
 ------------------------------------------------------------------------------
 Total: 1

 Attack Source Port Table:
 ------------------------------------------------------
  InterfaceName        Vlan:Outer/Inner       TOTAL
 ------------------------------------------------------
 Ethernet2/0/0              199/299            1264
 ------------------------------------------------------
 Total: 1

 Attack Source IP Table:
 ---------------------------------------
 IPAddress        TOTAL Packets
 ---------------------------------------
 10.105.105.2     256
 ---------------------------------------
 Total: 1
```

Display detailed information about the attack source list.

```
<Huawei> display auto-defend attack-source detail
 Attack Source User Table:
```

```
-------------------------------------------------------
MAC Address                 0000-0000-0023
Interface                  Ethernet2/0/0
VLAN: Outer/Inner            199/299
   ARP:                    256
Total                      256
-------------------------------------------------------
Total: 1

Attack Source Port Table:
-------------------------------------------------------
  InterfaceName       Vlan:Outer/Inner       TOTAL
-------------------------------------------------------
Ethernet2/0/0           199/299             256
-------------------------------------------------------
Total: 1

Attack Source IP Table:
-------------------------------------------------------
IP address                 10.105.105.2
   ARP:                    256
Total                      256
-------------------------------------------------------
Total: 1
```

Table 19-133 Description of the **display auto-defend attack-source** command output

Item	Description
Attack Source User Table	Information about attack sources on the SRU, which is distinguished according to the attack user.
Attack Source Port Table	Information about attack sources on the SRU. The attack source information is distinguished according to the attacked interface.
Attack Source IP Table	Information about attack sources on the SRU. The attack source information is distinguished according to the attacked interface.
MacAddress	MAC address of the user.
InterfaceName	Interface name.
Vlan:Outer/Inner	ID of the VLAN that an interface belongs to. **Outer** indicates the outer VLAN ID and **Inner** indicates the inner VLAN ID.
TOTAL	Total number of packets.
IPAddress	IP address of a user.
TOTAL Packets	Total number of packets.

Related Topics

19.10.11 cpu-defend policy

19.10.2 auto-defend enable

 Copyright © Huawei Technologies Co., Ltd.

19.10.16 display auto-defend configuration

Function

The **display auto-defend configuration** command displays the attack source tracing configuration.

Format

display auto-defend configuration [**cpu-defend policy** *policy-name*]

Parameters

Parameter	Description	Value
cpu-defend policy *policy-name*	Displays the attack source tracing configuration of a specified attack defense policy. • If this parameter is specified, the configuration of the specified attack defense policy is displayed. • If this parameter is not specified, the configurations of all attack defense policies are displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After attack source tracing is configured in an attack defense policy, you can run the **display auto-defend configuration** command to view the attack source tracing configuration.

Example

Display the configurations of all attack defense policies.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display auto-defend configuration
------------------------------------------------------------------------------
Name  : mypolicy
Related slot : <0>
auto-defend                : enable
auto-defend threshold      : 200 (pps)
auto-defend alarm          : enable
auto-defend alarm threshold : 2000 (pps)
------------------------------------------------------------------------------
Name  : mypolicy1
Related slot : <>
auto-defend                : enable
auto-defend threshold      : 128 (pps)
------------------------------------------------------------------------------
```

Table 19-134 Description of the display auto-defend configuration command output

Item	Description
Name	Name of an attack defense policy.
Related slot	ID of the slot to which the attack defense policy is applied.
auto-defend	Whether attack source tracing is enabled. To enable attack source tracing, run the **19.10.2 auto-defend enable** command.
auto-defend threshold	Checking threshold for attack source tracing. To set the checking threshold for attack source tracing, run the **19.10.7 auto-defend threshold** command.
auto-defend alarm	Whether the alarm function for attack source tracing is enabled. To enable the alarm function for attack source tracing, run the **19.10.4 auto-defend alarm enable** command.
auto-defend alarm threshold	Alarm threshold for attack source tracing. To set the alarm threshold for attack source tracing, run the **19.10.5 auto-defend alarm threshold** command.

Related Topics

19.10.11 cpu-defend policy
19.10.3 auto-defend action
19.10.4 auto-defend alarm enable
19.10.5 auto-defend alarm threshold
19.10.2 auto-defend enable
19.10.6 auto-defend protocol
19.10.8 auto-defend trace-type
19.10.7 auto-defend threshold

 Copyright © Huawei Technologies Co., Ltd.

19.10.17 display cpu-defend configuration

Function

The **display cpu-defend configuration** command displays rate limits for protocol packets.

Format

display cpu-defend configuration [**packet-type** *packet-type*] { **all** | **slot** *slot-id* | **sru** }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a packet type.	The supported packet type depends on the device.
all	Indicates all boards, including main control boards and LPUs.	-
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.
sru	Indicates the main control board. If **sru** is specified, the rate limit configuration on the SRU is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cpu-defend configuration** command to view the rate limit of protocol packets sent to the CPU. By default, the rate limit of protocol packets in the **default** policy is displayed.

Example

Display rate limit configuration about protocol packets sent to the SRU.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display cpu-defend configuration sru
Rate configurations on main board.
------------------------------------------------------------------------
Packet-type            Status       Rate-limit(PPS)  Priority
------------------------------------------------------------------------
8021X                  Disabled       160              2
arp-miss               Enabled         64              2
arp-reply              Enabled        128              2
arp-request            Enabled        128              2
bfd                    Disabled       512              4
bgp                    Enabled        256              3
......
------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 19-135 Description of the **display cpu-defend configuration** command output

Item	Description
Packet-type	Packet type.
Status	Protocol packet status.
Rate-limit(PPS)	Rate limit for packets, in pps. To set the rate limit for packets, run the **19.10.21 packet-type** command.
Priority	Priority of the protocol type. To set the priority of the protocol type, run the **19.10.22 packet-type priority** command.

19.10.18 display cpu-defend policy

Function

The **display cpu-defend policy** command displays the attack defense policy configuration.

Format

display cpu-defend policy [*policy-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Displays the configuration of a specified attack defense policy. • If *policy-name* is specified, information about the specified attack defense policy is displayed. • If *policy-name* is not specified, information about all attack defense policies is displayed.	The attack defense policy must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an attack defense policy is created, you can run the **display cpu-defend policy** command to view the board that the attack defense policy is applied to and configurations of the attack defense policy.

Example

Display information about the attack defense policy named **mypolicy**.

```
<Huawei> display cpu-defend policy mypolicy
 Related slot : <0>
 BlackList Status :
   Slot<0> : Success
 Configuration :
   Blacklist 1 ACL number : 2001
   Packet-type arp-reply rate-limit : 1260(pps)
   Packet-type arp-reply priority : 3
   Rate-limit all-packets : 12600(pps)
   Dynamic Rate-limit all-packets : 0(pps)
   Application-apperceive packet-type ftp : 1260(pps)
   Application-apperceive packet-type tftp : 1260(pps)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-136 Description of the display cpu-defend policy command output

Item	Description
Related slot	Board to which the attack defense policy is applied.
BlackList Status	Status of a blacklist.
Slot<0> : Success	A blacklist is successfully configured on the LPU in slot 0.
Blacklist 1 ACL number	Number of an ACL defined in blacklist 1. To configure a blacklist, run the **blacklist** command.
Packet-type arp-reply rate-limit	Rate limit for ARP Reply packets. To set the rate limit for ARP Reply packets, run the **packet-type** command.
Packet-type arp-reply priority	Priority of ARP Reply packets. To set the priority of ARP Reply packets, run the **packet-type priority** command.
Rate-limit all-packets	Rate limit for all packets sent to the CPU. To set the rate limit for all packets sent to the CPU, run the **rate-limit all-packets** command.
Dynamic Rate-limit all-packets	Dynamic rate limit for all packets sent to the CPU.
Application-apperceive packet-type ftp	Rate limit for FTP packets after ALP is enabled. To set the rate limit for FTP packets after ALP is enabled, run the **application-apperceive** command.
Application-apperceive packet-type tftp	Rate limit for TFTP packets after ALP is enabled.

Related Topics

19.10.9 blacklist
19.10.10 cpu-defend application-apperceive enable
19.10.11 cpu-defend policy
19.10.13 deny
19.10.14 description (attack defense policy view)

 Copyright © Huawei Technologies Co., Ltd.

19.10.19 display cpu-defend rate-adaption statistics

Function

The **display cpu-defend rate-adaption statistics** command displays packet statistics after CPCAR values are dynamically adjusted.

Format

display cpu-defend rate-adaption statistics [**packet-type** *packet-type*]

Parameters

Parameter	Description	Value
packet-type *packet-type*	Displays statistics on the specified type of protocol packets. • If *packet-type* is specified, statistics on the specified type of protocol packets are displayed. • If *packet-type* is not specified, statistics on all protocol packets are displayed.	The supported packet types depend on the device model.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view packet statistics after CPCAR values are dynamically adjusted, run this command. The displayed packet statistics, including protocol types, rate of passed packets, rate of discarded packets, and packet rate limit, help you configure attack defense policies.

Example

Display packet statistics after CPCAR values are dynamically adjusted.

```
<Huawei> display cpu-defend rate-adaption statistics
-------------------------------------------------------------------------------
Packet Type                Pass          Loss       Rate-limit
                          (pps)         (pps)        (pps)
-------------------------------------------------------------------------------
8021X                        0             0          128
arp-miss                     0             0           64
arp-reply                    0             0          128
arp-request                  0             0          128
bfd                          0             0          512
bgp                          0             0          256
......
```

 Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------------
```

Table 19-137 Description of the **display cpu-defend rate-adaption statistics** command output

Item	Description
Packet Type	Packet type.
Pass	Rate of passed packets, in pps.
Loss	Rate of discarded packets, in pps.
Rate-limit(PPS)	Packet rate limit, in pps.

19.10.20 display cpu-defend statistics

Function

The **display cpu-defend statistics** command displays statistics on packets sent to the CPU.

Format

display cpu-defend statistics [**packet-type** *packet-type*]

Parameters

Parameter	Description	Value
packet-type *packet-type*	Displays statistics on the specified type of protocol packets. *packet-type* specifies the packet type. • If *packet-type* is specified, statistics on the specified type of protocol packets are displayed. • If *packet-type* is not specified, statistics on all protocol packets are displayed.	The supported packet type depends on the device.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The **display cpu-defend statistics** command displays statistics on packets sent to the CPU, including the number of forwarded and discarded packets. This helps the network administrator configure attack defense policies.

Example

Display the statistics on packets sent to the main control board.

```
<Huawei> display cpu-defend statistics
-------------------------------------------------------------------------
Packet Type             Pass Packets        Drop Packets
-------------------------------------------------------------------------
8021X                          0                   0
arp-miss                       5                   0
arp-reply                   8090                   0
arp-request              1446576              127773
bfd                            0                   0
bgp                            0                   0
bgp4plus                       0                   0
dhcp-client                  879                   0
dhcp-server                    0                   0
dhcpv6-reply                   0                   0
dhcpv6-request                 0                   0
dlsw                           0                   0
dns                            4                   0
fib-hit                        0                   0
fr                             0                   0
ftp-client                     0                   0
ftp-server                     0                   0
fw-dns                         0                   0
fw-ftp                         0                   0
fw-http                        0                   0
fw-rtsp                        0                   0
fw-sip                         0                   0
gre-keepalive                  0                   0
gvrp                           0                   0
hdlc                           0                   0
http-client                    0                   0
http-server                    0                   0
hw-tacacs                      0                   0
icmp                          59                   0
icmpv6                       224                   0
igmp                         539                   0
ip-option                      0                   0
ipsec-ike                      0                   0
ipsec-isa                      0                   0
ipsec-osa                      0                   0
isis                       70252                   0
l2tp                           0                   0
lacp                           0                   0
lldp                           0                   0
ldp                            0                   0
nd                           358                   0
nd-miss                        0                   0
nhrp                           0                   0
ntp                            0                   0
ospf                           0                   0
ospfv3                         0                   0
pim                            0                   0
ppp                            0                   0
pppoe                          0                   0
```

 Copyright © Huawei Technologies Co., Ltd.

```
radius                          0                0
rip                         11306                0
ripng                        7385                0
snmp                            0                0
ssh-client                      0                0
ssh-server                      0                0
sslvpn                          0                0
stp                             0                0
tcp                            15                0
telnet-client                81476                0
telnet-server                   0                0
ttl-expired                     0                0
udp-helper                      0                0
unknown-multicast               0                0
unknown-packet              66146                0
voice                           0                0
vrrp                            0                0
------------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 19-138 Description of the **display cpu-defend statistics** command output

Item	Description
Packet Type	Packet type.
Pass Packets	Number of forwarded packets.
Drop Packets	Number of discarded packets.

Related Topics

19.10.30 reset cpu-defend statistics

19.10.21 packet-type

Function

The **packet-type** command sets the rate limit for packets sent to the CPU.

The **undo packet-type** command restores the default rate limit for packets sent to the CPU.

By default, the default rate limit in the **default** attack defense policy is used to limit the packets sent to the CPU.

Format

packet-type *packet-type* **rate-limit** *rate-value*

undo packet-type *packet-type* **rate-limit**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
packet-type	Specifies the protocol type.	The supported packet type depends on the device.
rate-limit *rate-value*	Specifies the rate limit of protocol packets.	The value is an integer that ranges from 1 to 32768, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an attack defense policy is created, if the device receives attack packets of a specified protocol or a large number of packets sent to the CPU, configure rate limit for the protocol packets in the attack defense policy. The device then limits the rate of these packets to protect the CPU.

By default, the device applies the rate limit defined in the **default** attack defense policy to protocol packets. You can also create an attack defense policy and run the **packet-type** command to set the rate limit of protocol packets. The configured rate limit overrides the default rate limit defined in the **default** attack defense policy.

Prerequisites

An attack defense policy has been created using the **cpu-defend policy** command.

Precautions

If you run the **packet-type** command with the same value of *packet-type* in the same attack defense policy view multiple times, only the latest configuration takes effect.

If the **packet-type** and **deny** commands are executed on the same type of protocol packets, the **deny** command takes effect.

Example

Set the rate limit for ARP Reply packets to 1260 pps in the attack defense policy named **mypolicy**.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] packet-type arp-reply rate-limit 1260
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.10.11 cpu-defend policy
19.10.13 deny
19.10.18 display cpu-defend policy
19.10.17 display cpu-defend configuration

19.10.22 packet-type priority

Function

The **packet-type priority** command sets a priority of protocol packets sent to the CPU.

The **undo packet-type** command restores the default priority for protocol packets sent to the CPU. The default priority is defined in the **default** attack defense policy.

By default, the priority defined in the **default** attack defense policy is used.

Format

packet-type *packet-type* **priority** *priority-level*

undo packet-type *packet-type* **priority**

Parameters

Parameter	Description	Value
packet-type	Sets a priority for packets of a specified protocol.	The supported packet type depends on the device.
priority *priority-level*	Specifies the priority.	The value is an integer that ranges from 1 to 4. A larger value indicates a higher priority.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

After an attack defense policy is created, set priorities of protocol packets in the attack defense policy so that packets with higher priorities are processed first.

By default, the priority of packets of a specified protocol type is set based on the **default** policy.

Precautions

If you run the **packet-type priority** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

You can create an attack defense policy and set the priority of packets of the specified protocol type using the **packet-type priority** command. The configured priority overrides the priority in the **default** policy.

The priority of protocol packets sent to the CPU configured in an attack defense policy takes effect only when the attack defense policy is applied to the main control board.

Example

Set the priority of ARP Reply packets to 3 in the attack defense policy named **mypolicy**.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] packet-type arp-reply priority 3
```

Related Topics

19.10.11 cpu-defend policy

19.10.18 display cpu-defend policy

19.10.17 display cpu-defend configuration

19.10.23 rate-adaption adjust-period

Function

The **rate-adaption adjust-period** command sets the interval for checking the CPU usage.

The **undo rate-adaption adjust-period** command restores the default interval for checking the CPU usage.

By default, the interval for checking CPU usage is 30 seconds.

Format

rate-adaption adjust-period *period-value*

undo rate-adaption adjust-period

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
period-value	Specifies the interval for checking CPU usage.	The value is an integer that ranges from 30 to 180, in seconds.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

If the CPU usage changes frequently, the device frequently adjusts CPCAR values, causing unstable traffic. To avoid this problem, run the **rate-adaption adjust-period** command to adjust the interval for checking CPU usage. Generally, use the default interval.

Example

Set the interval for checking CPU usage to 50 seconds.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption adjust-period 50
```

Related Topics

19.10.11 cpu-defend policy

19.10.24 rate-adaption adjust-step

Function

The **rate-adaption adjust-step** command sets the dynamic CPCAR adjustment step.

The **undo rate-adaption adjust-step** command restores the default dynamic CPCAR adjustment step.

By default, the dynamic CPCAR adjustment step is 20%.

Format

rate-adaption adjust-step *step-value*

undo rate-adaption adjust-step

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
step-value	Specifies the percentage value of dynamic CPCAR adjustment step. For example, if the adjustment step is 30% and the current CPCAR value is 1000 pps, the device reduces the CPCAR value to 700 pps when CPU usage reaches the upper threshold.	The value is an integer that ranges from 1 to 100.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

After dynamic CPCAR adjustment is enabled, the device checks the CPU usage at intervals. When the device detects that the CPU usage exceeds the upper threshold (set by the **rate-adaption cpu-usage threshold** command), and reduces the CPCAR value based on the step set by the **rate-adaption adjust-step** command to reduce CPU usage. Generally, the default step value can be used.

Example

Set the dynamic CPCAR adjustment step to 40%.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption adjust-step 40
```

Related Topics

19.10.11 cpu-defend policy

19.10.25 rate-adaption cpu-usage threshold

19.10.25 rate-adaption cpu-usage threshold

Function

The **rate-adaption cpu-usage threshold** command sets the CPU usage thresholds. When the CPU usage of a device exceeds the upper threshold or falls below the lower threshold, the device adjusts the CPCAR values.

The **undo rate-adaption cpu-usage threshold** command restores the default CPU usage thresholds.

By default, the lower threshold is 65% and the upper threshold is 85%.

 Copyright © Huawei Technologies Co., Ltd.

Format

rate-adaption cpu-usage threshold low *low-value* **high** *high-value*

undo rate-adaption cpu-usage threshold

Parameters

Parameter	Description	Value
low *low-value*	Specifies the lower CPU usage threshold. When the CPU usage of a device falls below the lower threshold, the device sets the CPCAR value to the default value or a manually set value.	The value is an integer that ranges from 1 to 99.
high *high-value*	Specifies the higher CPU usage threshold. When the CPU usage of a device exceeds the upper threshold, the device reduces the CPCAR value based on the step set by the **rate-adaption adjust-step** command.	The value is an integer that ranges from *low-value* +1 to 100. The value of *high-value* must be larger than the value of *low-value*.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

After dynamic CPCAR adjustment is configured, the device checks CPU usage to determine whether an attack occurs. When the CPU usage exceeds the upper threshold, the device reduces the CPCAR value based on the step set by the **rate-adaption adjust-step** command to reduce CPU load. When the CPU usage of a device falls below the lower threshold, the device sets the CPCAR value to the default value or a manually set value.

Example

Set the CPU usage thresholds for dynamic CPCAR adjustment.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption cpu-usage threshold low 40 high 90
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.10.11 cpu-defend policy
19.10.24 rate-adaption adjust-step

19.10.26 rate-adaption enable

Function

The **rate-adaption enable** command enables dynamic CPCAR adjustment.

The **undo rate-adaption enable** command disables dynamic CPCAR adjustment.

By default, dynamic CPCAR adjustment is disabled.

Format

rate-adaption enable

undo rate-adaption enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When CPCAR values are manually set, a device cannot immediately control the rate of packets sent to the CPU when undergoing an attack. As a result, the CPU usage exceeds the acceptable range and CPU performance degrades.

After dynamic CPCAR adjustment is configured, the device periodically checks CPU usage, and automatically adjusts CPCAR values of protocol packets when the CPU usage exceeds the specified upper threshold, reducing impact on the CPU.

Precautions

After dynamic CPCAR adjustment is enabled, the CPCAR values set using the **packet-type** command become invalid.

Example

Enable dynamic CPCAR adjustment.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.10.11 cpu-defend policy

19.10.21 packet-type

19.10.27 rate-adaption exception packet-type

Function

The **rate-adaption exception packet-type** command specifies the types of protocol packets for which the CPCAR values cannot be dynamically adjusted.

The **undo rate-adaption exception packet-type** command cancels the types of protocol packets for which the CPCAR values cannot be dynamically adjusted.

By default, the CPCAR values for all protocol packets are dynamically adjusted.

Format

rate-adaption exception packet-type *packet-type*

undo rate-adaption exception packet-type *packet-type*

Parameters

Parameter	Description	Value
packet-type	Specifies the protocol type.	The supported packet type depends on the device.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent certain protocol packets from being affected by dynamic CPCAR adjustment, for example, Telnet packets, you can run the **rate-adaption exception packet-type** command to specify the protected protocol packets. After this command is executed, dynamic CPCAR adjustment does not take effect for the protected protocol packets and you can specify rate limits for these packets by using the **packet-type** command.

Precautions

A maximum of eight types of protected protocol packets can be specified.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the types of protocol packets for which the CPCAR values cannot be dynamically adjusted.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption exception packet-type icmp
```

Related Topics

19.10.11 cpu-defend policy

19.10.21 packet-type

19.10.28 rate-limit all-packets

Function

The **rate-limit all-packets** command sets the rate limit for all packets sent to the CPU.

The **undo rate-limit all-packets** command restores the default rate limit for all packets sent to the CPU.

By default, the rate limit for all packets sent to the CPU is as follows:

- AR100&AR120&AR150&AR160&AR200 series: 1000pps
- AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, and AR2204: 1000pps
- AR2220, AR2240C: 1500pps
- AR2204XE, and AR2204XE-DC: 2000pps
- For the AR2240 and AR3260, the rate limit for all packets sent to the CPU depending on different SRUs.
  - SRU40: 1500pps
  - SRU80 and SRU100E: 2000pps
  - SRU200, SRU200E, and SRU400: 2500pps
- AR3600: 2500pps

Format

rate-limit all-packets pps *pps-value*

undo rate-limit all-packets pps

Parameters

Parameter	Description	Value
pps *pps-value*	Specifies the rate limit for all packets sent to the CPU.	The value is an integer that ranges from 500 to 65535, in pps.

Copyright © Huawei Technologies Co., Ltd.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an attack defense policy is created, you can limit the rate of all packet sent to the CPU in the attack defense policy. The device randomly discards packets that exceed the rate limit to ensure CPU security.

Precautions

If you run the **rate-limit all-packets** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

The priority of protocol packets sent to the CPU configured in an attack defense policy takes effect only when the attack defense policy is applied to the main control board.

Example

Set the rate limit for all packets sent to the CPU to 12600 pps in the attack defense policy named **mypolicy**.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-limit all-packets pps 12600
```

Related Topics

19.10.11 cpu-defend policy
19.10.18 display cpu-defend policy
19.10.17 display cpu-defend configuration

19.10.29 reset auto-defend attack-source

Function

The **reset auto-defend attack-source** command clears information about attack sources.

Format

reset auto-defend attack-source

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the latest attack source information on the device, run the **reset auto-defend attack-source** command to delete the existing attack source information, wait for a period, and run the **display auto-defend attack-source** command.

Precautions

After the **reset auto-defend attack-source** command is run, information about attack sources is cleared and cannot be restored.

Example

Delete existing attack source information on the device.

```
<Huawei> reset auto-defend attack-source
```

Related Topics

19.10.15 display auto-defend attack-source

19.10.30 reset cpu-defend statistics

Function

The **reset cpu-defend statistics** command clears statistics on packets sent to the CPU.

Format

reset cpu-defend statistics [**packet-type** *packet-type*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the protocol type of packets. *packet-type* specifies the packet type. • If **packet-type** *packet-type* is specified, the statistics on the specified type of protocol packets are cleared. • If **packet-type** *packet-type* is not specified, the statistics on all protocol packets are cleared.	The supported packet type depends on the device.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view statistics on the packets sent to the CPU in a specified period, run the **reset cpu-defend statistics** command to clear existing statistics and run the **display cpu-defend statistics** command.

Precautions

The deleted packet statistics cannot be restored.

Example

Clear statistics on BGP packets on the main control board.

```
<Huawei> reset cpu-defend statistics packet-type bgp
```

Related Topics

19.10.20 display cpu-defend statistics

19.11 Attack Defense Configuration Commands

19.11.1 anti-attack abnormal enable

Function

The **anti-attack abnormal enable** command enables defense against malformed packet attacks.

 Copyright © Huawei Technologies Co., Ltd.

The **undo anti-attack abnormal enable** command disables defense against malformed packet attacks.

The **anti-attack abnormal disable** command disables defense against malformed packet attacks.

By default, defense against malformed packet attacks is enabled.

Format

anti-attack abnormal enable

undo anti-attack abnormal enable

anti-attack abnormal disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The malformed packet attack is to send malformed IP packets to the system. If such an attack occurs, the system may break down when processing the malformed IP packets. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack abnormal enable** command to enable defense against malformed packets.

The device detects malformed packets after defense against malformed packets is enabled.

The device directly discards packets of the following types:

- Flood attacks from IP null payload packets
- Attacks from IGMP null payload packets
- LAND attacks
- Smurf attacks
- Attacks from packets with invalid TCP flag bits

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including malformed packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable defense against malformed packet attacks.

```
<Huawei> system-view
[Huawei] anti-attack abnormal enable
```

Related Topics

19.11.2 anti-attack enable

19.11.2 anti-attack enable

Function

The **anti-attack enable** command enables defense against all attack packets.

The **undo anti-attack enable** command disables defense against all attack packets.

The **anti-attack disable** command disables defense against all attack packets.

By default, defense against all attack packets is enabled.

Format

anti-attack enable

undo anti-attack enable

anti-attack disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different types of attacks on a network cause high device usage or system breakdown, affecting network services. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack enable** command to enable defense against all attack packets.

Precautions

Running the **anti-attack enable** command is equivalent to running all of the following commands:

 Copyright © Huawei Technologies Co., Ltd.

- **anti-attack abnormal enable**
- **anti-attack fragment enable**
- **anti-attack tcp-syn enable**
- **anti-attack udp-flood enable**
- **anti-attack icmp-flood enable**

Example

Enable defense against all attack packets.

```
<Huawei> system-view
[Huawei] anti-attack enable
```

Related Topics

19.11.1 anti-attack abnormal enable
19.11.3 anti-attack fragment enable
19.11.7 anti-attack tcp-syn enable
19.11.9 anti-attack udp-flood enable
19.11.5 anti-attack icmp-flood enable

19.11.3 anti-attack fragment enable

Function

The **anti-attack fragment enable** command enables defense against packet fragment attacks.

The **undo anti-attack fragment enable** command disables defense against packet fragment attacks.

The **anti-attack fragment disable** command disables defense against packet fragment attacks.

By default, defense against packet fragment attacks is enabled.

Format

anti-attack fragment enable

undo anti-attack fragment enable

anti-attack fragment disable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends error packet fragments to a device, the device consumes a large number of resources to process the error packet fragments, affecting normal services. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack fragment enable** command to enable defense against packet fragment attacks.

The device detects error packet fragments after defense against error packet fragments is enabled. If the device detects error packet fragments, the device limits the rate of these fragments to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including packet fragments.

Example

Enable defense against packet fragment attacks.

```
<Huawei> system-view
[Huawei] anti-attack fragment enable
```

Related Topics

19.11.2 anti-attack enable

19.11.4 anti-attack fragment car

Function

The **anti-attack fragment car** command sets the rate limit of packet fragments.

The **undo anti-attack fragment car** command restores the rate limit of packet fragments.

By default, the rate limit of packet fragments is 155000000 bit/s.

Format

anti-attack fragment car cir *cir*

undo anti-attack fragment car

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) of packet fragments.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against packet fragment attacks is enabled, run the **anti-attack fragment car** command to set the rate limit of packet fragments. If the rate of received packet fragments exceeds the rate limit, the device discards excess packet fragments to ensure that the device CPU works properly.

Prerequisites

Defense against packet fragment attacks has been enabled using the **anti-attack fragment enable** command.

Example

Set the rate limit of packet fragments to 8000 bit/s.

```
<Huawei> system-view
[Huawei] anti-attack fragment enable
[Huawei] anti-attack fragment car cir 8000
```

Related Topics

19.11.5 anti-attack icmp-flood enable

19.11.5 anti-attack icmp-flood enable

Function

The **anti-attack icmp-flood enable** command enables defense against ICMP flood attacks.

The **undo anti-attack icmp-flood enable** command disables defense against ICMP flood attacks.

The **anti-attack icmp-flood disable** command disables defense against ICMP flood attacks.

 Copyright © Huawei Technologies Co., Ltd.

By default, defense against ICMP flood attacks is enabled.

Format

anti-attack icmp-flood enable

undo anti-attack icmp-flood enable

anti-attack icmp-flood disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends a large number of ICMP request packets to the target host in a short time, the target host is busy with these ICMP request packets. As a result, the target host is overloaded and cannot process normal services. To prevent ICMP flood attacks, run the **anti-attack icmp-flood enable** command to enable defense against ICMP flood attacks.

The device detects ICMP flood attack packets after defense against ICMP flood attacks is enabled. If the device detects ICMP flood attack packets, the device limits the rate of these ICMP flood attack packets to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including ICMP flood attack packets.

Example

Enable defense against ICMP flood attacks.

```
<Huawei> system-view
[Huawei] anti-attack icmp-flood enable
```

Related Topics

19.11.6 anti-attack icmp-flood car

19.11.2 anti-attack enable

19.11.6 anti-attack icmp-flood car

 Copyright © Huawei Technologies Co., Ltd.

Function

The **anti-attack icmp-flood car** command sets the rate limit of ICMP flood attack packets.

The **undo anti-attack icmp-flood car** command restores the default rate limit of ICMP flood attack packets.

By default, the rate limit of ICMP flood attack packets is 155000000 bit/s.

Format

anti-attack icmp-flood car cir *cir*

undo anti-attack icmp-flood car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) of ICMP flood attack packets.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against ICMP flood attacks is enabled, run the **anti-attack icmp-flood car** command to set the rate limit of ICMP flood attack packets. If the rate of received ICMP flood attack packets exceeds the rate limit, the device discards excess ICMP flood attack packets to ensure that its CPU works properly.

Prerequisites

Defense against ICMP flood attacks has been enabled using the **anti-attack icmp-flood enable** command.

Example

Set the rate limit of ICMP flood attack packets to 8000 bit/s.

```
<Huawei> system-view
[Huawei] anti-attack icmp-flood enable
[Huawei] anti-attack icmp-flood car cir 8000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.11.5 anti-attack icmp-flood enable

19.11.7 anti-attack tcp-syn enable

Function

The **anti-attack tcp-syn enable** command enables defense against TCP SYN flood attacks.

The **undo anti-attack tcp-syn enable** command disables defense against TCP SYN flood attacks.

The **anti-attack tcp-syn disable** command disables defense against TCP SYN flood attacks.

By default, defense against TCP SYN flood attacks is enabled.

Format

anti-attack tcp-syn enable

undo anti-attack tcp-syn enable

anti-attack tcp-syn disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An attacker sends a SYN packet to a target host to initiate a TCP connection but does not respond to the SYN-ACK sent from the target host. If the target host receives no ACK packet from the attacker, it keeps waiting for the ACK packet. A half-open connection is formed. The attacker keeps sending SYN packets, so many half-open connections are set up on the target host. This wastes a large number of resources. To prevent TCP SYN flood attacks, run the **anti-attack tcp-syn enable** command to enable defense against TCP SYN flood attacks.

The device detects TCP SYN flood attack packets after defense against TCP SYN flood attacks is enabled. If the device detects TCP SYN flood attack packets, the device limits the rate of these TCP SYN flood attack packets to ensure that the device CPU works properly.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including TCP SYN flood attack packets.

Example

Enable defense against TCP SYN flood attacks.

```
<Huawei> system-view
[Huawei] anti-attack tcp-syn enable
```

Related Topics

19.11.8 anti-attack tcp-syn car

19.11.2 anti-attack enable

19.11.8 anti-attack tcp-syn car

Function

The **anti-attack tcp-syn car** command sets the rate limit at which TCP SYN packets are received.

The **undo anti-attack tcp-syn car** command restores the default rate limit at which TCP SYN packets are received.

By default, the rate limit at which TCP SYN packets are received is 155000000 bit/s.

Format

anti-attack tcp-syn car cir *cir*

undo anti-attack tcp-syn car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) at which TCP SYN packets are received.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After defense against TCP SYN flood attacks is enabled, run the **anti-attack tcp-syn car** command to set the rate limit at which TCP SYN packets are received. If the rate of received TCP SYN attack packets exceeds the rate limit, the device discards excess TCP SYN flood attack packets to ensure that the device CPU works properly.

Prerequisites

Defense against TCP SYN flood attacks has been enabled using the **anti-attack tcp-syn enable** command.

Example

Set the rate limit at which TCP SYN packets are received to 8000 bit/s.

```
<Huawei> system-view
[Huawei] anti-attack tcp-syn enable
[Huawei] anti-attack tcp-syn car cir 8000
```

Related Topics

19.11.7 anti-attack tcp-syn enable

19.11.9 anti-attack udp-flood enable

Function

The **anti-attack udp-flood enable** command enables defense against UDP flood attacks.

The **undo anti-attack udp-flood enable** command disables defense against UDP flood attacks.

The **anti-attack udp-flood disable** command disables defense against UDP flood attacks.

By default, defense against UDP flood attacks is enabled.

Format

anti-attack udp-flood enable

undo anti-attack udp-flood enable

anti-attack udp-flood disable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends a large number of UDP packets to the target host in a short time, the target host is busy with these UDP packets. As a result, the target host is overloaded and cannot process normal services. To prevent UDP flood attacks, run the **anti-attack udp-flood enable** command to enable defense against UDP flood attacks.

The device detects UDP flood attack packets after defense against UDP flood attacks is enabled. The device directly discards UDP flood attack packets.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including UDP flood attack packets.

Example

Enable defense against UDP flood attacks.

```
<Huawei> system-view
[Huawei] anti-attack udp-flood enable
```

Related Topics

19.11.2 anti-attack enable

19.11.10 anti-attack urpf

Function

The **anti-attack urpf** command enables URPF.

The **undo anti-attack urpf** command disables URPF.

By default, URPF is disabled.

Format

anti-attack urpf { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]

undo anti-attack urpf

Parameters

Parameter	Description	Value
loose	Indicates URPF loose check.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
strict	Indicates URPF strict check.	-
allow-default-route	Allows special processing of default routes.	-
acl *acl-number*	Specifies the ACL number.	The number is an integer ranging from 2000 to 3999. For the basic ACL, the number ranges from 2000 to 2999; for the advanced ACL, the number ranges from 3000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To ensure that the packets pass the URPF check when the forwarding table contains the related entries even if the interface that actually receives the packets does not match the outbound interface in the forwarding table, set the URPF check mode to **loose**. To ensure that the packets pass the URPF check only when the forwarding table contains related entries and the interface actually receives the packets matches the outbound interface in the forwarding table, set the URPF check mode to **strict**.

Example

Create ACL 2999, enable strict URPF check, and configure the device to allow special processing of default routes.

```
<Huawei> system-view
[Huawei] anti-attack urpf strict allow-default-route acl 2999
```

Related Topics

19.11.11 display anti-attack statistics

19.11.11 display anti-attack statistics

Function

The **display anti-attack statistics** command displays statistics about attack packets of a specified type.

If no parameter is specified, the **display anti-attack statistics** command displays statistics about attack packets of all types.

 Copyright © Huawei Technologies Co., Ltd.

Format

display anti-attack statistics [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood** | **urpf**]

Parameters

Parameter	Description	Value
abnormal	Displays statistics about malformed packets.	-
fragment	Displays statistics about defense against packet fragments.	-
tcp-syn	Displays statistics about defense against TCP SYN flood attacks.	-
udp-flood	Displays statistics about defense against UDP flood attacks.	-
icmp-flood	Displays statistics about defense against ICMP flood attacks.	-
urpf	Displays the statistics about URPF check.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display anti-attack statistics** command displays statistics on attack packets of the following types: malformed packet attack, packet fragment attack, TCP SYN flood attack, UDP flood attack, ICMP flood attack.

Example

Display attack defense statistics.

```
<Huawei> display anti-attack statistics
Packets Statistic Information:
------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum       DropPacketNum        PassPacketNum
             (H)       (L)       (H)       (L)       (H)       (L)
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
URPF          0        1088       0          0          0          1088
Abnormal      0        0          0          0          0          0
Fragment      0        0          0          0          0          0
Tcp-syn       0        58         0          0          0          58
Udp-flood     0        0          0          0          0          0
Icmp-flood    0        0          0          0          0          0
------------------------------------------------------------------------------
```

Table 19-139 Description of the display anti-attack statistics command output

Item	Description
AntiAtkType	Attack defense type: • URPF: URPF check • Abnormal: defense against malformed packets • Fragment: defense against packet fragments • Tcp-syn: defense against TCP SYN flood attacks • Udp-flood: defense against UDP flood attacks • Icmp-flood: defense against ICMP flood attacks
TotalPacketNum	Total number of packets.
DropPacketNum	Number of discarded packets.
PassPacketNum	Number of forwarded packets.
(H)	Highest-order bit display.
(L)	Lowest-order bit display.

Related Topics

19.11.12 reset anti-attack statistics

19.11.12 reset anti-attack statistics

Function

The **reset anti-attack statistics** command clears attack defense statistics.

Format

reset anti-attack statistics [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood** | **urpf**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
abnormal	Clears statistics about defense against malformed packets.	-
fragment	Clears statistics about defense against packet fragments.	-
tcp-syn	Clears statistics about defense against TCP SYN flood attacks.	-
udp-flood	Clears statistics about defense against UDP flood attacks.	-
icmp-flood	Clears statistics about defense against ICMP flood attacks.	-
urpf	Clears statistics about URPF check.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

If no attack defense is specified, statistics about all types of attack defense are cleared.

NOTICE

The cleared statistics cannot be restored. Exercise caution when you use the command.

Example

Clear statistics about defense against malformed packets.

```
<Huawei> reset anti-attack statistics abnormal
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.11.11 display anti-attack statistics

19.12 Traffic Suppression Configuration Commands

19.12.1 broadcast-suppression (interface view)

Function

The **broadcast-suppression** command sets the maximum traffic rate of broadcast packets that can pass through an interface.

The **undo broadcast-suppression** command cancels the rate limit for broadcast traffic on an interface.

By default, broadcast traffic is not suppressed on an interface.

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, 9ES2 board do not support traffic suppression on interfaces.

This command is not supported by the AR100 series, AR120 series, AR161, AR161W, AR161G-L, AR169, AR169W, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, AR161G-U, AR161G-Lc, AR161EW, AR161EW-M1, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR161FW-P-M5.

Format

broadcast-suppression { **cir** *cir-value* | **packets** *packets-per-second* }

undo broadcast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer, in kbit/s. The value range is as follows: • Fast Ethernet interface: 64 to 100000. • GE interface: 64 to 1000000. • XGE interface: 64 to 10000000.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
packets *packets-per-second*	Specifies the rate limit in number of packets per second (pps).	The value is an integer, in pps. The value range is as follows: • Fast Ethernet interface: 0 to 148810. • GE interface: 0 to 1488100. • XGE interface: 0 to 14881000.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

The accumulating broadcast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

To prevent broadcast storms, you can use the **broadcast-suppression** command to set the threshold of broadcast traffic that an interface allows to pass through. When the broadcast traffic rate reaches the rate limit, the system discards excess broadcast packets to control the traffic rate in a proper range.

Precautions

AR1220E, AR1220EV and AR1220EVW only supports the broadcast-suppression command, but does not support the multicast-suppression or unicast-suppression command.

Different types of interfaces support different modes for traffic suppression:

- The CIR value for traffic suppression can be set on the LAN-side Ethernet interfaces of the main control board.
- The rate limit in pps can be set on the LAN-side Ethernet interfaces of the LPU.

Different models support different types of interfaces and therefore different traffic suppression modes. Set the traffic suppression mode depending on the actual device configuration.

Example

Set the rate limit for broadcast traffic to 21600 pps on Ethernet 2/0/0

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] broadcast-suppression packets 21600
```

Related Topics

19.12.7 multicast-suppression (interface view)

19.12.9 unicast-suppression (interface view)

19.12.2 broadcast-suppression (system view)

Function

The **broadcast-suppression** command sets the maximum traffic rate of broadcast packets that can pass through an interface of a device.

The **undo broadcast-suppression** command cancels the rate limiting on the broadcast packets that can pass through an interface of a device.

By default, an interface of a device does not suppress broadcast packets.

NOTE

Only the AR161EW, AR161EW-M1, AR169EW, or AR169EGW-L support this command.

Format

broadcast-suppression cir *cir-value*

undo broadcast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The accumulating broadcast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

 Copyright © Huawei Technologies Co., Ltd.

To prevent broadcast storms, you can use the **broadcast-suppression** command to set the threshold of broadcast traffic that an interface of a device allows to pass through. When the broadcast traffic rate reaches the maximum value, the system discards excess broadcast packets to control the traffic volume in a proper range.

Storm control is a simple traffic suppression approach. Although the token bucket technology is used, the bucket depth is a fixed multiple of the traffic rate and cannot be changed. As a result, the size of broadcast traffic affects the time when storm control takes effect. After the **broadcast-suppression** command is run to set the maximum rate of broadcast packets that can pass through an interface of a device, storm control takes effect at a certain interval if the traffic entering the device is small. If the traffic is heavy, storm control takes effect immediately.

Example

Set the maximum rate of broadcast packets that can pass through an interface of a device to 50000 kbit/s.

```
<Huawei> system-view
[Huawei] broadcast-suppression cir 50000
```

Related Topics

19.12.8 multicast-suppression (system view)

19.12.10 unicast-suppression (system view)

19.12.3 display flow-suppression interface

Function

The **display flow-suppression interface** command displays the traffic suppression configuration on an interface.

Format

display flow-suppression interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. • *interface-type* specifies the type of the interface. • *interface-number* specifies the interface number.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the traffic suppression configuration on Ethernet 2/0/0.

```
<Huawei> display flow-suppression interface ethernet 2/0/0
 storm type         rate mode   set rate value
--------------------------------------------------------------------------------
 unknown-unicast    pps         pps: 1260(packet/s)
 multicast          pps         pps: 2520(packet/s)
 broadcast          pps         pps: 1260(packet/s)
--------------------------------------------------------------------------------
```

Display the traffic suppression configuration on Ethernet 0/0/0.

```
<Huawei> display flow-suppression interface ethernet 0/0/0
 storm type         rate mode   set rate value
--------------------------------------------------------------------------------
 unknown-unicast    bps         cir: 100(kbit/s)
 multicast          bps         cir: 200(kbit/s)
 broadcast          bps         cir: 100(kbit/s)
--------------------------------------------------------------------------------
```

Table 19-140 Description of the display flow-suppression interface command output

Item	Description
storm type	Traffic type. Broadcast traffic, multicast traffic, and unknown unicast traffic can be suppressed.
rate mode	Type of the rate limit. • bps: cir mode • pps: packet mode
set rate value	Configured rate limit.

Related Topics

19.12.1 broadcast-suppression (interface view)
19.12.7 multicast-suppression (interface view)
19.12.9 unicast-suppression (interface view)

19.12.4 flood-suppression (interface view)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **flood-suppression** command sets the maximum rate of broadcast, multicast, and unknown unicast packets that can pass through an interface.

The **undo flood-suppression** command cancels the rate limiting for broadcast, multicast, and unknown unicast packets on interfaces.

By default, the rate of broadcast, multicast, and unknown unicast packets on interfaces is not limited.

NOTE

Only the AR1220E, AR1220EV, and AR1220EVW support this command.

Format

flood-suppression cir *cir-value*

undo flood-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer and the unit is kbit/s. • For an Fast Ethernet interface, the value ranges from 64 to 100000. • For a GE interface, the value ranges from 64 to 1000000. • For an XGE interface, the value ranges from 64 to 10000000.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

The accumulating broadcast, multicast, and unknown unicast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

 Copyright © Huawei Technologies Co., Ltd.

To prevent broadcast storms, you can use the **flood-suppression** command to set the threshold of broadcast, multicast, and unknown unicast traffic that an interface allows to pass through. When the total traffic rate of broadcast, multicast, and unknown unicast traffic on an interface reaches the rate limit, the system discards excess packets to control the traffic rate in a proper range.

Example

Set the maximum rate of broadcast, multicast, and unknown unicast packets that can pass an interface to 50000 kbit/s.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/3
[Huawei-GigabitEthernet0/0/3] flood-suppression cir 50000
```

19.12.5 icmp rate-limit

Function

Using the **icmp rate-limit** command, you can configure the rate limit for ICMP packets globally or on an interface.

Using the **undo icmp rate-limit** command, you can restore the default rate limit for ICMP packets.

By default, the global rate limit and rate limit on an interface are both 100 pps.

Format

icmp rate-limit threshold *threshold-value*

undo icmp rate-limit threshold

Parameters

Parameter	Description	Value
threshold *threshold-value*	Indicates the rate limit for ICMP packets.	The value is an integer ranging from 1 to 32768, in pps.

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

 Copyright © Huawei Technologies Co., Ltd.

Before configuring the rate limit for ICMP packets, enable the Router to limit the rate of incoming ICMP packets by using the **icmp rate-limit enable** command.

The Router can be configured to limit the rate of incoming ICMP packets globally or on an interface, and discard excess ICMP packets when the rate of incoming ICMP packets exceeds the limit.

You can run the **icmp rate-limit** command to set a global rate limit for ICMP packets and run this command in multiple interface views to limit the rate of ICMP packets on these interfaces. The total rate of ICMP packets on all the interfaces cannot exceed the global rate limit.

Precautions

To make suppression of ICMP packets take effect, disable the fast ICMP reply function.

The **undo icmp rate-limit** command cannot be configured in the system view.

Example

Set the rate limit for ICMP packets on Eth 2/0/0 to 20 pps.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] icmp rate-limit threshold 20
```

Related Topics

19.12.6 icmp rate-limit enable

19.12.6 icmp rate-limit enable

Function

The **icmp rate-limit enable** command enables the traffic suppression function for ICMP packets.

The **undo icmp rate-limit enable** command disables the traffic suppression function for ICMP packets.

By default, the traffic suppression function for ICMP packets is disabled.

Format

icmp rate-limit enable

undo icmp rate-limit enable

Parameters

None

Views

System view, GE interface view, XGE interface view, Ethernet interface view, Eth-Trunk interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Attackers may send a large number of ICMP packets to attack a network. If the device sends all the received ICMP packets to the CPU for processing, a lot of CPU usage resources are occupied and other services may be abnormal. To prevent ICMP packet attacks, you can configure the device to suppress ICMP packets.

After you run the **icmp rate-limit enable** command in the system view or interface view, the device limits the rate of ICMP packets by the default traffic suppression.

You can then run the **icmp rate-limit** command in the system view or interface view to configure a traffic suppression for ICMP packets.

Example

Enable the traffic suppression function for ICMP packets.

```
<Huawei> system-view
[Huawei] icmp rate-limit enable
```

Related Topics

19.12.5 icmp rate-limit

19.12.7 multicast-suppression (interface view)

Function

The **multicast-suppression** command sets the maximum traffic volume of multicast packets that can pass through an interface.

Using the **undo multicast-suppression** command, you can cancel the rate limit for multicast traffic on an interface.

By default, multicast traffic is not suppressed on an interface.

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, 9ES2 board do not support traffic suppression on interfaces.

This command is not supported by the AR100 series, AR120 series, AR161, AR161W, AR161G-L, AR169, AR169W, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, AR161G-U, AR161G-Lc, AR161EW, AR161EW-M1, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR161FW-P-M5.

Format

multicast-suppression { **cir** *cir-value* | **packets** *packets-per-second* }

undo multicast-suppression

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer, in kbit/s. The value range is as follows: ● Fast Ethernet interface: 64 to 100000. ● GE interface: 64 to 1000000. ● XGE interface: 64 to 10000000.
packets *packets-per-second*	Specifies the rate limit in number of packets per second (pps).	The value is an integer, in pps. The value range is as follows: ● Fast Ethernet interface: 0 to 148810. ● GE interface: 0 to 1488100. ● XGE interface: 0 to 14881000.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

When an increasing number of multicast packets are transmitted on a network, more network resources are occupied and services are affected.

To prevent broadcast storms, you can use the **multicast-suppression** command to set the threshold of multicast traffic that an interface allows to pass through. When the multicast traffic volume exceeds the threshold, the system discards the excess multicast packets to control the traffic volume of multicast packets to a proper range.

Precautions

Different types of interfaces support different modes for traffic suppression:

- The CIR value for traffic suppression can be set on the LAN-side Ethernet interfaces of the main control board.

 Copyright © Huawei Technologies Co., Ltd.

- The rate limit in pps can be set on the LAN-side Ethernet interfaces of the LPU.

Different models support different types of interfaces and therefore different traffic suppression modes. Set the traffic suppression mode depending on the actual device configuration.

Example

Set the rate limit for multicast traffic to 21600 pps on Ethernet 2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] multicast-suppression cir 21600
```

Related Topics

19.12.1 broadcast-suppression (interface view)

19.12.9 unicast-suppression (interface view)

19.12.8 multicast-suppression (system view)

Function

The **multicast-suppression** command sets the maximum traffic rate of multicast packets that can pass through an interface of a device.

The **undo multicast-suppression** command cancels the rate limiting on the multicast packets that can pass through an interface of a device.

By default, an interface of a device does not suppress multicast packets.

NOTE

Only the AR161EW, AR161EW-M1, AR169EW, or AR169EGW-L support this command.

Format

multicast-suppression cir *cir-value*

undo multicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The accumulating multicast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

To prevent broadcast storms, you can use the **multicast-suppression** command to set the threshold of multicast traffic that an interface of a device allows to pass through. When the multicast traffic volume reaches the threshold, the system discards the excessive multicast packets to control the traffic volume of multicast packets in to a proper range.

Storm control is a simple traffic suppression approach. Although the token bucket technology is used, the bucket depth is a fixed multiple of the traffic rate and cannot be changed. As a result, the size of multicast traffic affects the time when storm control takes effect. After the **multicast-suppression** command is run to set the maximum rate of multicast packets that can pass through an interface of a device, storm control takes effect at a certain interval if the traffic entering the device is small. If the traffic is heavy, storm control takes effect immediately.

Example

Set the maximum rate of multicast packets that can pass through an interface of a device to 50000 kbit/s.

```
<Huawei> system-view
[Huawei] multicast-suppression cir 50000
```

Related Topics

19.12.2 broadcast-suppression (system view)

19.12.10 unicast-suppression (system view)

19.12.9 unicast-suppression (interface view)

Function

The **unicast-suppression** command sets the maximum traffic volume of unknown unicast packets that can pass through an interface.

Using the **undo unicast-suppression** command, you can cancel the rate limit for unicast traffic on an interface.

By default, unicast traffic is not suppressed on an interface.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, 9ES2 board do not support traffic suppression on interfaces.

This command is not supported by the AR100 series, AR120 series, AR161, AR161W, AR161G-L, AR169, AR169W, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, AR161G-U, AR161G-Lc, AR161EW, AR161EW-M1, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR161FW-P-M5.

Format

unicast-suppression { **cir** *cir-value* | **packets** *packets-per-second* }

undo unicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer, in kbit/s. The value range is as follows: • Fast Ethernet interface: 64 to 100000. • GE interface: 64 to 1000000. • XGE interface: 64 to 10000000.
packets *packets-per-second*	Specifies the rate limit in number of packets per second (pps).	The value is an integer, in pps. The value range is as follows: • Fast Ethernet interface: 0 to 148810. • GE interface: 0 to 1488100. • XGE interface: 0 to 14881000.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

 Copyright © Huawei Technologies Co., Ltd.

When an increasing number of unknown multicast packets are transmitted on the network, more network resources are occupied and services are affected.

To prevent broadcast storms, you can use the **unicast-suppression** command to set the threshold of unicast traffic that an interface allows to pass through. When the unknown unicast traffic rate exceeds the rate limit, the system discards excess unknown unicast packets to control the traffic volume in a proper range.

Precautions

Different types of interfaces support different modes for traffic suppression:

- The CIR value for traffic suppression can be set on the LAN-side Ethernet interfaces of the main control board.
- The rate limit in pps can be set on the LAN-side Ethernet interfaces of the LPU.

Different models support different types of interfaces and therefore different traffic suppression modes. Set the traffic suppression mode depending on the actual device configuration.

Example

Set the rate limit for unknown unicast traffic to 21600 pps on Ethernet 2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] unicast-suppression packets 21600
```

Related Topics

19.12.1 broadcast-suppression (interface view)

19.12.7 multicast-suppression (interface view)

19.12.10 unicast-suppression (system view)

Function

The **unicast-suppression** command sets the maximum traffic rate of unknown unicast packets that can pass through an interface of a device.

The **undo unicast-suppression** command cancels the rate limiting on the unknown unicast packets that can pass through an interface of a device.

By default, an interface of a device does not suppress unknown unicast packets.

NOTE

Only the AR161EW, AR161EW-M1, AR169EW, or AR169EGW-L support this command.

Format

unicast-suppression cir *cir-value*

undo unicast-suppression

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The accumulating unknown unicast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

To prevent broadcast storms, you can use the **unicast-suppression** command to set the threshold of unknown unicast traffic that an interface of a device allows to pass through. When the unknown unicast traffic rate reaches the rate limit, the system discards excess unknown unicast packets to control the traffic volume in a proper range.

Storm control is a simple traffic suppression approach. Although the token bucket technology is used, the bucket depth is a fixed multiple of the traffic rate and cannot be changed. As a result, the size of unicast traffic affects the time when storm control takes effect. After the **unicast-suppression** command is run to set the maximum rate of unicast packets that can pass through an interface of a device, storm control takes effect at a certain interval if the traffic entering the device is small. If the traffic is heavy, storm control takes effect immediately.

Example

Set the maximum rate of unknown unicast packets that can pass through an interface of a device to 50000 kbit/s.

```
<Huawei> system-view
[Huawei] unicast-suppression cir 50000
```

Related Topics

19.12.2 broadcast-suppression (system view)

19.12.8 multicast-suppression (system view)

19.13 ARP Security Configuration Commands

 Copyright © Huawei Technologies Co., Ltd.

19.13.1 arp anti-attack check user-bind alarm enable

Function

The **arp anti-attack check user-bind alarm enable** command enables the alarm function for ARP packets discarded by DAI.

The **undo arp anti-attack check user-bind alarm enable** command disables the alarm function for ARP packets discarded by DAI.

By default, the alarm function for ARP packets discarded by DAI is disabled.

Format

arp anti-attack check user-bind alarm enable

undo arp anti-attack check user-bind alarm enable

Parameters

None

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DAI is enabled, if you want to receive an alarm when a large number of ARP packets are discarded by DAI, you can run the **arp anti-attack check user-bind alarm enable** command. After the alarm function is enabled, the device sends an alarm when the number of discarded ARP packets exceeds the threshold.

The alarm threshold is set by the **19.13.2 arp anti-attack check user-bind alarm threshold** command.

Prerequisites

DAI has been enabled on the interface using the **arp anti-attack check user-bind enable** command.

Precautions

Since the default interval for sending ARP alarms is 0 (that is, no ARP alarm is sent), you must run the **arp anti-attack log-trap-timer** *time* command to increase the alarm sending interval after enabling the alarm for packets discarded by DAI.

This command can be used only on Layer 2 interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the alarm function for ARP packets discarded by DAI on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind enable
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind alarm enable
```

Related Topics

19.13.5 arp anti-attack check user-bind enable

19.13.2 arp anti-attack check user-bind alarm threshold

19.13.2 arp anti-attack check user-bind alarm threshold

Function

The **arp anti-attack check user-bind alarm threshold** command sets the alarm threshold for ARP packets discarded by DAI.

The **undo arp anti-attack check user-bind alarm threshold** command restores the default alarm threshold for ARP packets discarded by DAI.

The threshold on interfaces is consistent with the threshold set by the **arp anti-attack check user-bind alarm threshold** command in the system view. If the alarm threshold is not set in the system view, the default threshold on the interface is 100.

Format

System view:

arp anti-attack check user-bind alarm threshold *threshold*

undo arp anti-attack check user-bind alarm threshold

Interface view:

arp anti-attack check user-bind alarm threshold *threshold*

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the ARP packets discarded by DAI.	The value is an integer that ranges from 1 to 1000.

Views

System view, Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can use this command to set the alarm threshold for ARP packets discarded by DAI. After the alarm threshold is set, the device sends an alarm when the number of ARP packets discarded by DAI exceeds this threshold.

Prerequisites

DAI has been enabled using the **arp anti-attack check user-bind enable** command in the interface view, and the alarm function for ARP packets discarded by DAI has been enabled using the **arp anti-attack check user-bind alarm enable** command.

Precautions

The **arp anti-attack check user-bind alarm threshold** command takes effect in the system view only when DAI and the alarm function for ARP packets discarded by DAI are enabled on the interface. The global alarm threshold takes effect on all interfaces enabled with the two functions.

If the alarm thresholds are set in the interface view and system view, the alarm threshold configured in the interface view takes effect. If the alarm threshold on an interface is not configured, the global alarm threshold is used.

The **arp anti-attack check user-bind alarm threshold** command can be used only on Layer 2 interfaces.

Example

Set the alarm threshold for ARP packets discarded by DAI on Eth2/0/0 to 200.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind enable
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind alarm enable
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind alarm threshold 200
```

Related Topics

19.13.5 arp anti-attack check user-bind enable

19.13.1 arp anti-attack check user-bind alarm enable

19.13.3 arp anti-attack check user-bind check-item (interface view)

Function

The **arp anti-attack check user-bind check-item** command configures check items for ARP packet check based on binding entries on an interface.

The **undo arp anti-attack check user-bind check-item** command restores the default check items.

By default, the check items consist of IP address, MAC address, and VLAN ID.

 Copyright © Huawei Technologies Co., Ltd.

Format

arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **vlan** } *

undo arp anti-attack check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Indicates that the device checks IP addresses in ARP packets.	-
mac-address	Indicates that the device checks MAC addresses in ARP packets.	-
vlan	Indicates that the device checks VLAN IDs in ARP packets.	-

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device receives an ARP packet, it compares the source IP address, source MAC address, and VLAN ID of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

To allow some special ARP packets that match only one or two items in binding entries to pass through, use the **arp anti-attack check user-bind check-item** command to configure the device to check ARP packets according to one or two specified items in binding entries.

Prerequisites

DAI has been enabled on the interface using the **arp anti-attack check user-bind enable** command.

Precautions

Check items configured for ARP packet check based on binding entries do not take effect on hosts that are configured with static binding entries. These hosts check ARP packets based on all items in static binding entries.

This command can be used only on Layer 2 interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure Eth2/0/0 to check IP addresses in ARP packets.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind enable
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind check-item ip-address
```

Related Topics

19.13.5 arp anti-attack check user-bind enable
19.13.4 arp anti-attack check user-bind check-item (VLAN view)

19.13.4 arp anti-attack check user-bind check-item (VLAN view)

Function

The **arp anti-attack check user-bind check-item** command configures check items for ARP packet check based on binding entries in a VLAN.

The **undo arp anti-attack check user-bind check-item** command restores the default check items.

By default, the check items consist of IP address, MAC address, and interface number.

Format

arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **interface** } *

undo arp anti-attack check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Indicates that the device checks IP addresses in ARP packets.	-
mac-address	Indicates that the device checks MAC addresses in ARP packets.	-
interface	Indicates that the device checks interface numbers in ARP packets.	-

Views

VLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a device receives an ARP packet, it compares the source IP address, source MAC address, and interface number of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

To allow some special ARP packets that match only one or two items in binding entries to pass through, configure the device to check ARP packets according to one or two specified items in binding entries.

Prerequisites

DAI has been enabled in the VLAN using the **arp anti-attack check user-bind enable** command.

Precautions

Check items configured for ARP packet check based on binding entries do not take effect on hosts that are configured with static binding entries. These hosts check ARP packets based on all items in static binding entries.

Example

Configure the device to check IP addresses in ARP packets from VLAN 100.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] arp anti-attack check user-bind enable
[Huawei-vlan100] arp anti-attack check user-bind check-item ip-address
```

Related Topics

19.13.5 arp anti-attack check user-bind enable

19.13.3 arp anti-attack check user-bind check-item (interface view)

19.13.5 arp anti-attack check user-bind enable

Function

The **arp anti-attack check user-bind enable** command enables DAI on an interface or in a VLAN. DAI enables the device to check ARP packets based on binding entries.

The **undo arp anti-attack check user-bind enable** command disables DAI on an interface or in a VLAN.

By default, DAI is disabled on an interface or in a VLAN.

Format

arp anti-attack check user-bind enable

undo arp anti-attack check user-bind enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent MITM attacks and theft on authorized user information, run the **arp anti-attack check user-bind enable** command to enable DAI. When a device receives an ARP packet, it compares the source IP address, source MAC address, VLAN ID, and interface number of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

You can enable DAI in the interface view or the VLAN view. When DAI is enabled in an interface view, the device checks all ARP packets received on the interface against binding entries. When DAI is enabled in the VLAN view, the device checks ARP packets received on interfaces belong to the VLAN based on binding entries.

This command can be used only on Layer 2 interfaces.

Follow-up Procedure

Run the **arp anti-attack check user-bind check-item (interface view)** or **arp anti-attack check user-bind check-item (VLAN view)** command to configure check items for ARP packet check based on binding entries.

Example

Enable DAI on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind enable
```

Enable DAI in VLAN 100.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] arp anti-attack check user-bind enable
```

Related Topics

19.13.3 arp anti-attack check user-bind check-item (interface view)

19.13.4 arp anti-attack check user-bind check-item (VLAN view)

19.13.6 arp anti-attack entry-check enable

 Copyright © Huawei Technologies Co., Ltd.

Function

The **arp anti-attack entry-check enable** command enables ARP entry fixing.

The **undo arp anti-attack entry-check enable** command disables ARP entry fixing.

By default, ARP entry fixing is disabled.

Format

arp anti-attack entry-check { **fixed-mac** | **fixed-all** | **send-ack** } **enable**

undo arp anti-attack entry-check enable

Parameters

Parameter	Description	Value
fixed-mac	Indicates ARP entry fixing in **fixed-mac** mode. When receiving an ARP packet, the device discards the packet if the MAC address does not match the MAC address in the corresponding ARP entry. If the MAC address in the ARP packet matches that in the corresponding ARP entry while the interface number or VLAN ID does not match that in the ARP entry, the device updates the interface number or VLAN ID in the ARP entry.	-
fixed-all	Indicates ARP entry fixing in **fixed-all** mode. When the MAC address, interface number, and VLAN ID of an ARP packet match those in the corresponding ARP entry, the device updates other information about the ARP entry.	-
send-ack	Indicates ARP entry fixing in **send-ack** mode. When the device receives an ARP packet with a changed MAC address, interface number, or VLAN ID, it does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address in the ARP entry, and then determines whether to change the MAC address, VLAN ID, or interface number in the ARP entry depending on the response from the user.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To defend against ARP address spoofing attacks, enable ARP entry fixing. The **fixed-mac**, **fixed-all**, and **send-ack** modes are applicable to different scenarios and are mutually exclusive:

- The **fixed-mac** mode applies to networks where user MAC addresses are unchanged but user access locations often change. When a user connects to a different interface on the device, the device updates interface information in the ARP entry of the user timely.
- The **fixed-all** mode applies to networks where user MAC addresses and user access locations are fixed.
- The **send-ack** mode applies to networks where user MAC addresses and user access locations often change.

Example

Enable ARP entry fixing and specify the **fixed-mac** mode.

```
<Huawei> system-view
[Huawei] arp anti-attack entry-check fixed-mac enable
```

Related Topics

19.13.31 display arp anti-attack configuration

19.13.7 arp anti-attack gateway-duplicate enable

Function

The **arp anti-attack gateway-duplicate enable** command enables ARP gateway anti-collision.

The **undo arp anti-attack gateway-duplicate enable** command disables ARP gateway anti-collision.

By default, ARP gateway anti-collision is disabled.

Format

arp anti-attack gateway-duplicate enable

undo arp anti-attack gateway-duplicate enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker forges the gateway address to send ARP packets with the source IP address being the IP address of the gateway on the LAN, ARP entries on hosts in the LAN record the incorrect gateway address. As a result, all traffic from user hosts to the gateway is sent to the attacker and the attacker intercepts user information. Communication of users is interrupted.

To prevent bogus gateway attacks, enable ARP gateway anti-collision on the gateway using the **arp anti-attack gateway-duplicate enable** command. The gateway considers that a gateway collision occurs when a received ARP packet meets either of the following conditions:

- The source IP address in the ARP packet is the same as the IP address of the VLANIF interface matching the physical inbound interface of the packet.
- The source IP address in the ARP packet is the virtual IP address of the inbound interface but the source MAC address in the ARP packet is not the virtual MAC address of the VRRP group.

The device generates an ARP anti-collision entry and discards the received packets with the same source MAC address and VLAN ID in a specified period. This function prevents ARP packets with the bogus gateway address from being broadcast in a VLAN.

Precautions

A maximum of 100 ARP anti-attack entries exist on the device at the same time. When the maximum number is exceeded, the device cannot prevent new ARP gateway collision attacks.

Example

Enable ARP gateway anti-collision.

```
<Huawei> system-view
[Huawei] arp anti-attack gateway-duplicate enable
```

Related Topics

19.13.31 display arp anti-attack configuration

19.13.32 display arp anti-attack gateway-duplicate item

19.13.8 arp anti-attack log-trap-timer

Function

The **arp anti-attack log-trap-timer** command sets the interval for sending ARP alarms.

The **undo arp anti-attack log-trap-timer** command restores the default setting.

 Copyright © Huawei Technologies Co., Ltd.

The default interval for sending alarms is 0, indicating that the device does not send ARP alarms.

Format

arp anti-attack log-trap-timer *time*

undo arp anti-attack log-trap-timer

Parameters

Parameter	Description	Value
time	Specifies the interval for sending ARP alarms.	The value is an integer that ranges from 0 to 1200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow the administrator to learn the ARP running status in real time, define potential attacks, and take measures, the device provides the alarm function for potential ARP attacks. This function records exceptions of ARP running in real time. To avoid excessive alarms when ARP attacks occur, reduce the alarm quantity by setting a proper interval for sending alarms.

NOTE

The **arp anti-attack log-trap-timer** command takes effect only on the following alarms:

- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.4 hwARPSDaiDropALarm
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.5 hwARPGlobleSpeedLimitALarm
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.8 hwARPMissGlobleSpeedLimitALarm
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.3 hwARPSPacketCheck
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.1 hwARPSGatewayConflict
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.2 hwARPSEntryCheck

Precautions

In the insecure environment, you are advised to extend the interval for sending ARP alarms. This prevents excessive ARP alarms. In the secure environment, you are advised to shorten the interval for sending ARP alarms. This facilitates fault rectification in real time.

After the interval is set, the device discards alarms generates in this interval; therefore, some faults cannot be rectified in real time.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval for sending ARP alarms to 20 seconds.

```
<Huawei> system-view
[Huawei] arp anti-attack log-trap-timer 20
```

Related Topics

19.13.31 display arp anti-attack configuration

19.13.9 arp anti-attack packet-check sender-mac

Function

The **arp anti-attack packet-check sender-mac** command checks whether the source MAC address in an ARP packet is the same as that in the Ethernet frame header.

The **undo arp anti-attack packet-check sender-mac** command disables ARP packet validity check.

By default, ARP packet validity check is disabled.

Format

arp anti-attack packet-check sender-mac

undo arp anti-attack packet-check sender-mac

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving an ARP packet, the device checks validity of the ARP packet, including:

- Packet length
- Validity of the source and destination MAC addresses in the ARP packet
- ARP Request type and ARP Reply type
- MAC address length
- IP address length

 Copyright © Huawei Technologies Co., Ltd.

- Whether the ARP packet is an Ethernet frame

The preceding check items are used to determine whether an ARP packet is valid. The packet with different source MAC addresses in the ARP packet and Ethernet frame header is possibly an attack packet although it is allowed by the ARP protocol. After the **arp anti-attack packet-check sender-mac** command is used, the device checks the source MAC addresses in the ARP packet and Ethernet frame header, and discards the packets with inconsistent source MAC addresses.

Precautions

The **arp validate** command can be used to configure the device to check whether the source MAC address in an ARP packet is the same as that in the Ethernet frame header. This command is different from the **arp anti-attack packet-check sender-mac** command.

- The **arp validate** command configures ARP packet validity check only on a physical interface. The **arp anti-attack packet-check sender-mac** command configures ARP packet validity check globally.
- The **arp validate** command checks whether the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header. The **arp anti-attack packet-check sender-mac** command checks whether the source MAC address in an ARP packet is the same as that in the Ethernet frame header.

Example

Enable ARP packet validity check to allow the device to check the source MAC address in an ARP packet.

```
<Huawei> system-view
[Huawei] arp anti-attack packet-check sender-mac
```

Related Topics

19.13.31 display arp anti-attack configuration

19.13.10 arp anti-attack rate-limit

Function

The **arp anti-attack rate-limit** command sets the maximum rate and rate limiting duration of ARP packets globally or on an interface.

The **undo arp anti-attack rate-limit** command restores the default maximum rate and rate limiting duration of ARP packets globally or on an interface.

By default, a maximum of 100 ARP packets are allowed to pass per second.

Format

arp anti-attack rate-limit *packet-number* [*interval-value*]

undo arp anti-attack rate-limit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
packet-number	Specifies the maximum rate of sending ARP packets, that is, the number of ARP packets allowed to pass through in the rate limiting duration.	The value is an integer that ranges from 1 to 32768. The default value is 100.
interval-value	Specifies the rate limiting duration of ARP packets.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 1 second.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP packets is enabled, run the **arp anti-attack rate-limit** command to set the maximum rate and rate limiting duration of ARP packets globally or on an interface. In the rate limiting duration, if the number of received ARP packets exceeds the limit, the device discards the excess ARP packets.

Prerequisites

Rate limit on ARP packets has been enabled globally or on an interface using the **arp anti-attack rate-limit enable** command.

Precautions

If the maximum rate and rate limiting duration are configured in the system view and interface view at the same time, the device uses the configurations in the interface view and system view in order.

Example

Configure Eth2/0/0 to allow 200 ARP packets to pass through in 10 seconds.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack rate-limit enable
[Huawei-Ethernet2/0/0] arp anti-attack rate-limit 200 10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.13.13 arp anti-attack rate-limit enable

19.13.11 arp anti-attack rate-limit alarm enable

Function

The **arp anti-attack rate-limit alarm enable** command enables the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit.

The **undo arp anti-attack rate-limit alarm enable** command disables the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit.

By default, the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit is disabled.

Format

arp anti-attack rate-limit alarm enable

undo arp anti-attack rate-limit alarm enable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP packets is enabled, if you want the device to generate alarms for excessive discarded ARP packets, run the **arp anti-attack rate-limit alarm enable** command. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

You can set the alarm threshold using the **arp anti-attack rate-limit alarm threshold** command.

Prerequisites

Rate limit on ARP packets has been enabled using the **arp anti-attack rate-limit enable** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After the **arp anti-attack rate-limit alarm enable** command is run, you need to run the **arp anti-attack log-trap-timer** *time* command to set the interval for sending alarms.

Example

Enable rate limit on ARP packets globally and enable the alarm function.

```
<Huawei> system-view
[Huawei] arp anti-attack rate-limit enable
[Huawei] arp anti-attack rate-limit alarm enable
```

Related Topics

19.13.13 arp anti-attack rate-limit enable

19.13.12 arp anti-attack rate-limit alarm threshold

19.13.12 arp anti-attack rate-limit alarm threshold

Function

The **arp anti-attack rate-limit alarm threshold** command sets the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit.

By default, the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit is 100.

Format

arp anti-attack rate-limit alarm threshold *threshold*

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit.	The value is an integer that ranges from 1 to 32768.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

You can use the **arp anti-attack rate-limit alarm threshold** command to set the alarm threshold. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

Prerequisites

Rate limit on ARP packets has been enabled using the **arp anti-attack rate-limit enable** command, and the alarm function has been enabled using the **arp anti-attack rate-limit alarm enable** command.

Example

Enable rate limit on ARP packets globally, enable the alarm function, and set the alarm threshold to 50.

```
<Huawei> system-view
[Huawei] arp anti-attack rate-limit enable
[Huawei] arp anti-attack rate-limit alarm enable
[Huawei] arp anti-attack rate-limit alarm threshold 50
```

Related Topics

19.13.13 arp anti-attack rate-limit enable

19.13.11 arp anti-attack rate-limit alarm enable

19.13.13 arp anti-attack rate-limit enable

Function

The **arp anti-attack rate-limit enable** command enables rate limit on ARP packets.

The **undo arp anti-attack rate-limit enable** command disables rate limit on ARP packets.

By default, rate limiting on ARP packet is disabled.

Format

arp anti-attack rate-limit enable

undo arp anti-attack rate-limit enable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The device has no sufficient CPU resource to process other services when processing a large number of ARP packets. To protect CPU resources of the device, limit the rate of ARP packets.

You can run the **arp anti-attack rate-limit enable** command to enable rate limit on ARP packets. When the rate of ARP packets exceeds the limit, excess ARP packets are discarded. To set the rate limit and rate limiting duration of ARP packets, run the **arp anti-attack rate-limit** command.

Example

Enable rate limit on ARP packets globally.

```
<Huawei> system-view
[Huawei] arp anti-attack rate-limit enable
```

Related Topics

19.13.10 arp anti-attack rate-limit

19.13.14 arp gratuitous-arp send enable

Function

The **arp gratuitous-arp send enable** command enables gratuitous ARP packet sending.

The **undo arp gratuitous-arp send enable** command disables gratuitous ARP packet sending.

By default, gratuitous ARP packet sending is disabled.

Format

arp gratuitous-arp send enable

undo arp gratuitous-arp send enable

Parameters

None

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

If an attacker forges the gateway address to send ARP packets to other user hosts, ARP entries on the hosts record the incorrect gateway address. As a result, the gateway cannot receive data sent from the hosts. You can enable gratuitous ARP packet sending on the gateway. Then the gateway sends gratuitous ARP packets at intervals to update the ARP entries of authorized users so that the ARP entries contain the correct MAC address of the gateway.

By default, the device sends a gratuitous ARP packet every 90 seconds after this function is enabled. You can also set the interval using the **arp gratuitous-arp send interval** command.

Precautions

After you run the **arp gratuitous-arp send enable** command in the system view, gratuitous ARP packet sending is enabled on all VLANIF interfaces. In addition, gratuitous ARP packet sending is enabled on all interfaces for the NAT address pool, NAT server, and public address for static NAT.

After you run the **undo arp gratuitous-arp send enable** command in the system view, gratuitous ARP packet sending is disabled on all VLANIF interfaces.

Example

Enable gratuitous ARP packet sending on VLANIF 10.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp gratuitous-arp send enable
```

Related Topics

19.13.15 arp gratuitous-arp send interval

19.13.15 arp gratuitous-arp send interval

Function

The **arp gratuitous-arp send interval** command sets the interval for sending gratuitous ARP packets.

The **undo arp gratuitous-arp send interval** command restores the default interval for sending gratuitous ARP packets.

By default, the interval for sending gratuitous ARP packets is 90 seconds.

Format

arp gratuitous-arp send interval *interval-time*

undo arp gratuitous-arp send interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for sending gratuitous ARP packets.	The value is an integer that ranges from 1 to 86400, in seconds.

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device sends a gratuitous ARP packet every 90 seconds after gratuitous ARP sending is enabled. You can set the interval for sending gratuitous ARP packets using the **arp gratuitous-arp send interval** command.

If you set the interval in the system view, the configuration takes effect on all VLANIF interfaces. If you set the interval in both the system view and VLANIF interface view, the configuration on the VLANIF interface takes precedence over the global configuration.

Prerequisites

Gratuitous ARP packet sending has been enabled using the **arp gratuitous-arp send enable** command.

Example

Set the interval for sending gratuitous ARP packets to 100 seconds on VLANIF 10.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp gratuitous-arp send enable
[Huawei-Vlanif10] arp gratuitous-arp send interval 100
```

Related Topics

19.13.14 arp gratuitous-arp send enable

19.13.16 arp learning dhcp-trigger

Function

The **arp learning dhcp-trigger** command enables ARP learning triggered by DHCP.

 Copyright © Huawei Technologies Co., Ltd.

The **undo arp learning dhcp-trigger** command disables ARP learning triggered by DHCP.

By default, ARP learning triggered by DHCP is disabled.

Format

arp learning dhcp-trigger

undo arp learning dhcp-trigger

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many DHCP users connect to a network device, the device needs to learn and maintain many ARP entries. This affects device performance.

To address this issue, configure ARP learning triggered by DHCP on the gateway. When the DHCP server allocates an IP address for a user, the gateway generates an ARP entry for the user based on the DHCP ACK packet received on the VLANIF interface.

Precautions

Before using this command, ensure that DHCP snooping is enabled using the **dhcp snooping enable** command.

When both VRRP and DHCP relay are configured on the network, neither the **dhcp snooping enable** command nor the **arp learning dhcp-trigger** command can be configured on the VRRP master and backup devices.

Example

Enable ARP learning triggered by DHCP on VLANIF 100.

```
<Huawei> system-view
[Huawei] vlan batch 100
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] arp learning dhcp-trigger
```

Related Topics

19.14.11 dhcp snooping enable

 Copyright © Huawei Technologies Co., Ltd.

19.13.17 arp learning strict (interface view)

Function

The **arp learning strict** command enables strict ARP learning on the interface.

The **undo arp learning strict** command restores the global configuration on the interface.

By default, the configuration of strict ARP learning is the same as the global configuration.

Format

arp learning strict { **force-enable** | **force-disable** | **trust** }

undo arp learning strict

Parameters

Parameter	Description	Value
force-enable	Indicates that strict ARP learning is enabled.	-
force-disable	Indicates that strict ARP learning is disabled.	-
trust	Indicates that the configuration of strict ARP learning is the same as the global configuration. **NOTE** The effect of the **trust** parameter is the same as the effect of the **undo arp learning strict** command.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many user hosts send a large number of ARP packets to a device simultaneously, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with each other.

 Copyright © Huawei Technologies Co., Ltd.

To avoid the preceding problems, enable strict ARP learning on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself, but does not allow the device to learn the ARP entries for the ARP packets received from other devices. In this way, the device can defend against most ARP attacks.

Precautions

The configuration on an interface takes precedence over the global configuration.

When ARP attacks occur on many interfaces of the device, you can run the **19.13.18 arp learning strict (system view)** command to enable strict ARP learning globally.

This command can be used only on Layer 3 interfaces.

Example

Enable strict ARP learning on VLANIF 100.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] arp learning strict force-enable
```

Related Topics

19.13.18 arp learning strict (system view)

19.13.34 display arp learning strict

19.13.18 arp learning strict (system view)

Function

The **arp learning strict** command enables strict ARP learning.

The **undo arp learning strict** command restores the default setting.

By default, strict ARP learning is disabled.

Format

arp learning strict

undo arp learning strict

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many user hosts send a large number of ARP packets to a device simultaneously, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with each other.

To avoid the preceding problems, enable strict ARP learning on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself. In this way, the device can defend against most ARP attacks.

Precautions

The configuration on an interface takes precedence over the global configuration.

Example

Enable strict ARP learning.

```
<Huawei> system-view
[Huawei] arp learning strict
```

Related Topics

19.13.17 arp learning strict (interface view)

19.13.34 display arp learning strict

19.13.19 arp speed-limit flood-rate

Function

The **arp speed-limit flood-rate** command sets the maximum rate of broadcasting ARP Request packets on VLANIF interfaces in all super-VLANs.

The **undo arp speed-limit flood-rate** command restores the default maximum rate of broadcasting ARP Request packets on VLANIF interfaces in all super-VLANs.

By default, the maximum rate of broadcasting ARP Request packets on VLANIF interfaces in all super-VLANs is 1000 pps.

Format

arp speed-limit flood-rate *rate*

 Copyright © Huawei Technologies Co., Ltd.

undo arp speed-limit flood-rate

Parameters

Parameter	Description	Value
rate	Specifies the maximum rate of broadcasting ARP Request packets.	The value is an integer that ranges from 0 to 32768, in pps. The value 0 indicates that the rate of broadcasting ARP packets is not limited.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A VLANIF interface in a super-VLAN is triggered to learn ARP entries in the following scenarios:

- The VLANIF interface receives IP packets triggering ARP Miss messages.
- The VLANIF interface is enabled with ARP proxy and receives ARP packets whose destination IP addresses meet the proxy requirements and match no ARP entry.

The VLANIF interface replicates ARP Request packets in each sub-VLAN when learning ARP entries. If a large number of sub-VLANs are configured for the super-VLAN, the device generates a large number of ARP Request packets. As a result, the CPU is busy processing ARP Request packets, and other services are affected. To prevent this problem, limit the rate of ARP packets on the VLANIF interface of a super-VLAN.

When the CPU is busy processing packets, set the maximum rate of broadcasting ARP Request packets to a small value. When the CPU is idle, set the maximum rate of broadcasting ARP Request packets to a large value to broadcast packets efficiently. You can set the maximum rate of broadcasting ARP Request packets based on the actual network environment.

Example

Set the maximum rate of broadcasting ARP Request packets on VLANIF interfaces in all super-VLANs to 500 pps.

```
<Huawei> system-view
[Huawei] arp speed-limit flood-rate 500
```

Related Topics

19.13.33 display arp flood statistics

 Copyright © Huawei Technologies Co., Ltd.

19.13.20 arp speed-limit source-mac

Function

The **arp speed-limit source-mac** command sets the maximum rate of ARP packets based on source MAC addresses.

The **undo arp speed-limit source-mac** command restores the default setting.

By default, the maximum rate of ARP packets from each source MAC address is set to 0, that is, the rate of ARP packets is not limited based on source MAC addresses.

Format

arp speed-limit source-mac [*mac-address*] **maximum** *maximum*

undo arp speed-limit source-mac [*mac-address*]

Parameters

Parameter	Description	Value
mac-address	Specifies the source MAC address. If this parameter is specified, the rate of ARP packets from the MAC address is limited. If this parameter is not specified, the rate of ARP packets from each MAC address is limited.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
maximum *maximum*	Specifies the maximum rate of ARP packets from a specified MAC address.	The value is an integer that ranges from 0 to 32768, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When processing a large number of ARP packets with fixed source MAC addresses but variable source IP addresses, the CPU is overloaded and ARP entries are exhausted. To prevent this problem, limit the rate of ARP packets based on source MAC addresses.

 Copyright © Huawei Technologies Co., Ltd.

After the **arp speed-limit source-mac** command is run, the device collects statistics on ARP packets from a specified source MAC address. If the number of ARP packets from a specified source IP address per second exceeds the threshold, the device discards the excess ARP packets.

Precautions

Limiting the rate of all ARP packets is not recommended. You are advised to find out the attack source according to packet statistics, and then limit the rate of ARP packets from the specified source MAC address.

Example

Set the maximum rate of ARP packets from any source MAC address to 100 pps.

```
<Huawei> system-view
[Huawei] arp speed-limit source-mac maximum 100
```

Set the maximum rate of ARP packets from a specified MAC address 0000-0000-0001 to 50 pps.

```
<Huawei> system-view
[Huawei] arp speed-limit source-mac 0000-0000-0001 maximum 50
```

Related Topics

19.13.21 arp speed-limit source-ip

19.13.31 display arp anti-attack configuration

19.13.21 arp speed-limit source-ip

Function

The **arp speed-limit source-ip** command sets the maximum rate of ARP packets based on the source IP address.

The **undo arp speed-limit source-ip** command restores the default setting.

By default, the device allows a maximum of 5 ARP packets from the same source IP address to pass through per second.

Format

arp speed-limit source-ip [*ip-address*] **maximum** *maximum*

undo arp speed-limit source-ip [*ip-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address. If this parameter is specified, the rate of ARP packets from the IP address is limited. If this parameter is not specified, the rate of ARP packets from each IP address is limited.	The value is in dotted decimal notation.
maximum *maximum*	Specifies the maximum rate of ARP packets from a specified source IP address. **NOTE** If the rate of all ARP packets is limited, a large value is recommended because valid packets may be discarded if the value is small. However, a too large value will deteriorate the system performance. If an IP address initiates attacks, you can set the maximum number of ARP Miss messages triggered by packets from this IP address to a small value.	The value is an integer that ranges from 0 to 32768, in pps. If the value is 0, the rate of ARP packets is not limited based on the source IP address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When processing a large number of ARP packets with fixed IP addresses (for example, the ARP packets with the same source IP addresses but frequently changing MAC addresses or outbound interfaces), the CPU is overloaded and cannot process other services. To prevent this problem, limit the rate of ARP packets based on the source IP address.

After the **arp speed-limit source-ip** command is run, the device collects statistics on ARP packets based on the source IP address. If the number of ARP packets from a specified source IP address per second exceeds the threshold, the device discards the excess ARP packets.

Precautions

Limiting the rate of all ARP packets is not recommended. You are advised to find out the attack source according to packet statistics, and then limit the rate of ARP packets from the specified source IP address.

Example

Set the maximum rate of ARP packets from a source IP address to 100 pps.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] arp speed-limit source-ip maximum 100
```

Set the maximum rate of ARP packets from a specified IP address 10.0.0.1 to 50 pps.

```
<Huawei> system-view
[Huawei] arp speed-limit source-ip 10.0.0.1 maximum 50
```

Related Topics

19.13.20 arp speed-limit source-mac
19.13.31 display arp anti-attack configuration

19.13.22 arp validate (interface view)

Function

The **arp validate** command enables MAC address consistency check in an ARP packet on an interface. This function compares the source and destination MAC addresses in ARP packets with those in the Ethernet frame header.

The **undo arp validate** command disables MAC address consistency check in an ARP packet on an interface.

By default, MAC address consistency check in an ARP packet is disabled.

Format

arp validate { **source-mac** | **destination-mac** } *

undo arp validate { **source-mac** | **destination-mac** } *

Parameters

Parameter	Description	Value
source-mac	Indicates that the device compares the source MAC address in a received ARP packet with that in the Ethernet frame header.	-
destination-mac	Indicates that the device compares the destination MAC address in a received ARP packet with that in the Ethernet frame header.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The MAC address consistency check function for ARP packets prevents attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header. This function is usually configured on gateways.

After the **arp validate** command is run, the gateway checks the MAC address consistency in an ARP packet before ARP learning. If the source and destination MAC addresses in an ARP packet are different from those in the Ethernet frame header, the device discards the packet as an attack. If the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header, the device performs ARP learning.

When using this command, note the following points:

- If **source-mac** is specified:
  - When receiving an ARP Request packet, the device checks only the source MAC address consistency.
  - When receiving an ARP Reply packet, the device checks only the source MAC address consistency.
- If **destination-mac** is specified:
  - When receiving an ARP Request packet, the device does not check the destination MAC address consistency because the ARP Request packet is broadcast.
  - When receiving an ARP Reply packet, the device checks the destination MAC address consistency.
- If **source-mac** and **destination-mac** are specified:
  - When receiving an ARP Request packet, the device checks only the source MAC address consistency.
  - When receiving an ARP Reply packet, the device checks the source and destination MAC address consistency.

Precautions

Sub-interfaces do not support the **arp validate** command. When receiving ARP packets, a sub-interface checks MAC address consistency based on the rule configured on the primary interface.

Example

Enable MAC address consistency check in an ARP packet on Layer 2 interface Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp validate source-mac destination-mac
```

19.13.23 arp-fake expire-time

Function

The **arp-fake expire-time** command sets the aging time of temporary ARP entries.

 Copyright © Huawei Technologies Co., Ltd.

The **undo arp-fake expire-time** command restores the default aging time of temporary ARP entries.

By default, the aging time of temporary ARP entries is 1 second.

Format

arp-fake expire-time *expire-time*

undo arp-fake expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time of temporary ARP entries.	The value is an integer that ranges from 1 to 36000, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, VLANIF interface view, port group view, virtual ethernet interface view

Default Level

2: Configuration level

Usage Guidelines

When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network.

- In the aging time of temporary ARP entries:
  - Before receiving an ARP reply packet, the device discards the IP packets matching the temporary ARP entry and does not generate ARP Miss messages.
  - After receiving an ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.
- When temporary ARP entries age out, the device clears them. If no ARP entry matches the IP packets forwarded by the device, ARP Miss messages and temporary ARP entries are repeatedly generated

When a device undergoes an ARP Miss attack, you can run the **arp-fake expire-time** command to extend the aging time of temporary ARP entries to reduce the frequency of triggering ARP Miss messages and minimize the impact on the device.

Example

Set the aging time of temporary ARP entries to 10 seconds on VLANIF10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] quit
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp-fake expire-time 10
```

 Copyright © Huawei Technologies Co., Ltd.

19.13.24 arp-limit

Function

The **arp-limit** command sets the maximum number of ARP entries that an interface can dynamically learn.

The **undo arp-limit** command deletes the maximum number of ARP entries that an interface can dynamically learn.

By default, the maximum number of ARP entries that an interface can dynamically learn is the maximum value that can be configured on the interface.

Format

VLANIF interface view

arp-limit maximum *maximum*

undo arp-limit

Other interface views

arp-limit vlan *vlan-id1* [**to** *vlan-id2*] **maximum** *maximum*

undo arp-limit vlan *vlan-id1* [**to** *vlan-id2*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the ID of a VLAN from which the maximum number of ARP entries an interface can dynamically learn is limited. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If **to** *vlan-id2* is not specified, the device limits the maximum number of ARP entries an interface dynamically learns from the VLAN *vlan-id1*. If **to** *vlan-id2* is specified, the device limits the maximum number of ARP entries an interface dynamically learns from	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	each VLAN from *vlan-id1* to *vlan-id2*.	
maximum *maximum*	Specifies the maximum number of ARP entries that an interface can dynamically learn.	The value is an integer and the value range varies according to product models: ● AR100&AR120&AR150&AR160&AR200&AR1200 series: 1 to 2000 ● AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204E, AR2204-51GE, AR2204-51GE-R, AR2204E-D and AR2204: 1 to 2000 ● AR2204XE, AR2204XE-DC, AR2220, AR2220E: 1 to 4000 ● AR2240 and AR2240C: 1 to 4000 ● AR3200 and AR3600 series: 1 to 4000 .

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent ARP entries from being exhausted by ARP attacks from a host connecting to an interface on the device, set the maximum number of ARP entries that the interface can dynamically learn. When the number of the ARP entries learned by a specified interface reaches the maximum number, no dynamic ARP entry can be added.

Precautions

If the number of ARP entries learned by an interface exceeds the maximum number, the device neither learns new ARP entries nor clears the learned ARP entries. Instead, the device asks users to delete the excess ARP entries.

 Copyright © Huawei Technologies Co., Ltd.

Ethernet, GE, VE, Eth-Trunk interfaces can work at Layer 3 or Layer 2. When they work at Layer 3, you cannot configure the VLAN ID. When they work at Layer 2, you must configure the VLAN ID.

If the **arp-limit vlan** *vlan-id1* **to** *vlan-id2* **maximum** *maximum* command is run more than once, the following situations are available:

- If **maximum** *maximum* is the same in multiple command instances, all configurations take effect. For example, if the **arp-limit vlan 10 to 30 maximum 200** command and then the **arp-limit vlan 35 to 40 maximum 200** command are run, both configurations take effect. If the VLAN ranges specified in multiple command instances are overlapping, the system automatically merges the VLAN ranges. For example, if the **arp-limit vlan 50 to 80 maximum 200** command and then the **arp-limit vlan 70 to 100 maximum 200** command are run, both configurations take effect, and the system merges the configurations into **arp-limit vlan 50 to 100 maximum 200**.
- If **maximum** *maximum* is different in multiple command instances, the latest configuration overrides the previous one for the same VLAN range. For example, if the **arp-limit vlan 10 to 30 maximum 200** command and then the **arp-limit vlan 15 to 25 maximum 300** command are run, the system automatically divides the configurations into **arp-limit vlan 10 to 14 maximum 200**, **arp-limit vlan 15 to 25 maximum 300**, and **arp-limit vlan 26 to 30 maximum 200**.

Example

Configure that VLANIF 10 can dynamically learn a maximum of 20 ARP entries.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] quit
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp-limit maximum 20
```

Configure that Eth2/0/0 can dynamically learn a maximum of 20 ARP entries corresponding to VLAN 10.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp-limit vlan 10 maximum 20
```

Related Topics

19.13.36 display arp-limit

19.13.25 arp-miss anti-attack rate-limit

Function

The **arp-miss anti-attack rate-limit** command sets the maximum rate and rate limiting duration of ARP Miss messages.

The **undo arp-miss anti-attack rate-limit** command restores the default maximum rate and rate limiting duration of ARP Miss messages.

By default, the device can process a maximum of 100 ARP Miss messages per second.

 Copyright © Huawei Technologies Co., Ltd.

Format

arp-miss anti-attack rate-limit *packet-number* [*interval-value*]

undo arp-miss anti-attack rate-limit

Parameters

Parameter	Description	Value
packet-number	Specifies the maximum rate of ARP Miss messages, that is, the number of ARP Miss messages the device processes in the rate limiting duration.	The value is an integer that ranges from 1 to 32768. The default value is 100.
interval-value	Specifies the rate limiting duration of ARP Miss messages.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 1 second.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP Miss messages is enabled, you can set maximum rate and rate limiting duration of ARP Miss messages. If the number of ARP Miss messages triggered by IP packets in the rate limiting duration exceeds the limit, the device does not process the excess ARP Miss packets and discards the IP packets triggering the excess ARP Miss messages.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command.

Example

Configure the device to process a maximum of 200 ARP Miss messages in 10 seconds.

```
<Huawei> system-view
[Huawei] arp-miss anti-attack rate-limit enable
[Huawei] arp-miss anti-attack rate-limit 200 10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.13.28 arp-miss anti-attack rate-limit enable

19.13.26 arp-miss anti-attack rate-limit alarm enable

Function

The **arp-miss anti-attack rate-limit alarm enable** command enables the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

The **undo arp-miss anti-attack rate-limit alarm enable** command disables the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

By default, the alarm function is disabled.

Format

arp-miss anti-attack rate-limit alarm enable

undo arp-miss anti-attack rate-limit alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP Miss messages is enabled, if you want that the device can generate alarms to notify the network administrator of a large number of discarded excess ARP Miss messages, run the **arp-miss anti-attack rate-limit alarm enable** command. When the number of discarded ARP Miss packets exceeds the alarm threshold, the device generates an alarm.

You can set the alarm threshold using the **arp-miss anti-attack rate-limit alarm threshold** command.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After the **arp-miss anti-attack rate-limit alarm enable** command is run, you need to run the **arp anti-attack log-trap-timer** *time* command to set the interval for sending alarms.

Example

Enable the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

```
<Huawei> system-view
[Huawei] arp-miss anti-attack rate-limit enable
[Huawei] arp-miss anti-attack rate-limit alarm enable
```

Related Topics

19.13.25 arp-miss anti-attack rate-limit

19.13.27 arp-miss anti-attack rate-limit alarm threshold

19.13.28 arp-miss anti-attack rate-limit enable

19.13.27 arp-miss anti-attack rate-limit alarm threshold

Function

The **arp-miss anti-attack rate-limit alarm threshold** command sets the alarm threshold for ARP Miss messages discarded when the rate of ARP Miss packets exceeds the limit.

By default, the alarm threshold for ARP Miss packets discarded is 100.

Format

arp-miss anti-attack rate-limit alarm threshold *threshold*

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.	The value is an integer that ranges from 1 to 32768.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can use the **arp-miss anti-attack rate-limit alarm threshold** command to set the alarm threshold. When the number of discarded ARP Miss packets exceeds the alarm threshold, the device generates an alarm.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command, and the alarm function has been enabled using the **arp-miss anti-attack rate-limit alarm enable** command.

Example

Enable rate limit on ARP Miss messages, enable the alarm function, and set the alarm threshold to 200.

```
<Huawei> system-view
[Huawei] arp-miss anti-attack rate-limit enable
[Huawei] arp-miss anti-attack rate-limit alarm enable
[Huawei] arp-miss anti-attack rate-limit alarm threshold 200
```

Related Topics

19.13.25 arp-miss anti-attack rate-limit

19.13.26 arp-miss anti-attack rate-limit alarm enable

19.13.28 arp-miss anti-attack rate-limit enable

19.13.28 arp-miss anti-attack rate-limit enable

Function

The **arp-miss anti-attack rate-limit enable** command enables rate limit on ARP Miss messages.

The **undo arp-miss anti-attack rate-limit enable** command disables rate limit on ARP Miss messages.

By default, rate limit on ARP Miss messages is disabled.

Format

arp-miss anti-attack rate-limit enable

undo arp-miss anti-attack rate-limit enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a host sends a large number of IP packets with unresolvable destination IP addresses to attack a device, that is, if the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route, the device triggers a large number of ARP Miss messages. IP packets triggering ARP Miss messages are sent to the control board for processing. The device generates a large number of temporary ARP entries and sends many ARP Request packets to the network, consuming a large number of CPU and bandwidth resources.

To avoid the preceding problems, configure rate limit on ARP Miss messages. The device collects statistics on ARP Miss messages. If the number of ARP Miss messages generated within the rate limiting duration exceeds the threshold (the maximum number of ARP Miss messages), the gateway discards the IP packets triggering the excess ARP Miss messages.

Follow-up Procedure

Run the **arp-miss anti-attack rate-limit** command to set the maximum rate and rate limiting duration of ARP Miss messages.

Example

Enable rate limit on ARP Miss messages.

```
<Huawei> system-view
[Huawei] arp-miss anti-attack rate-limit enable
```

Related Topics

19.13.25 arp-miss anti-attack rate-limit

19.13.29 arp-miss speed-limit source-ip

Function

The **arp-miss speed-limit source-ip** command sets the maximum number of ARP Miss messages based on source IP addresses.

The **undo arp-miss speed-limit source-ip** command restores the default setting.

By default, the device processes a maximum of 5 ARP Miss messages triggered by IP packets from the same source IP address per second.

Format

arp-miss speed-limit source-ip [*ip-address*] **maximum** *maximum*

undo arp-miss speed-limit source-ip [*ip-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address. If this parameter is specified, the maximum number of ARP Miss messages triggered by packets from this IP address is limited. If this parameter is not specified, the maximum number of ARP Miss messages triggered by packets from each IP address is limited.	The value is in dotted decimal notation.
maximum *maximum*	Specifies the maximum number of ARP Miss messages based on the source IP address. **NOTE** If the maximum number of ARP Miss messages triggered by packets from each IP address is limited, a large value is recommended for this parameter because a small value may cause discarding of valid packets. However, a too large value will deteriorate the system performance. If an IP address initiates attacks, you can set the maximum number of ARP Miss messages triggered by packets from this IP address to a small value.	The value is an integer that ranges from 0 to 32768. If the value is 0, the maximum number of ARP Miss messages is not limited based on the source IP address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the device considers that an attack is initiated from the source IP address. The administrator can use the **arp-miss speed-limit source-ip** command to set the maximum number of ARP Miss messages that the device can process within a specified duration, protecting the system resources and ensuring proper running of other services.

Example

Set the maximum number of ARP Miss messages triggered by each source IP address per second to 60.

```
<Huawei> system-view
[Huawei] arp-miss speed-limit source-ip maximum 60
```

 Copyright © Huawei Technologies Co., Ltd.

Set the maximum number of ARP Miss messages triggered by the IP address 10.0.0.1 per second to 100, and set the maximum number of ARP Miss messages triggered by other source IP addresses per second to 60.

```
<Huawei> system-view
[Huawei] arp-miss speed-limit source-ip maximum 60
[Huawei] arp-miss speed-limit source-ip 10.0.0.1 maximum 100
```

Related Topics

19.13.31 display arp anti-attack configuration

19.13.30 display arp anti-attack check user-bind interface

Function

The **display arp anti-attack check user-bind interface** command displays the configuration of ARP packet check on an interface.

Format

display arp anti-attack check user-bind interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where ARP packets are checked. Where, • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp anti-attack check user-bind interface** command to view the configuration of ARP packet check on an interface, including whether the

 Copyright © Huawei Technologies Co., Ltd.

function is enabled, check items, whether the alarm function is enabled for discarded ARP packets, alarm threshold, and number of discarded ARP packets.

Only after DAI and the alarm function are enabled, output of this command is displayed.

Example

Display ARP check configuration on Eth2/0/0.

```
<Huawei> display arp anti-attack check user-bind interface ethernet 2/0/0
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 50
 ARP packet drop count = 0
```

Table 19-141 Description of the **display arp anti-attack check user-bind interface** command output

Item	Description
arp anti-attack check user-bind enable	DAI has been enabled on an interface. You can run the **19.13.5 arp anti-attack check user-bind enable** command to enable DAI.
arp anti-attack check user-bind alarm enable	The alarm function for ARP packets discarded by DAI has been enabled. You can run the **19.13.1 arp anti-attack check user-bind alarm enable** command to enable the alarm function.
arp anti-attack check user-bind alarm threshold 50	Alarm threshold of discarded ARP packets matching no DHCP snooping binding entry. You can run the **19.13.2 arp anti-attack check user-bind alarm threshold** command to set the alarm threshold.
ARP packet drop count	Number of discarded ARP packets matching no DHCP snooping binding entry.

Related Topics

19.13.5 arp anti-attack check user-bind enable

19.13.1 arp anti-attack check user-bind alarm enable

19.13.2 arp anti-attack check user-bind alarm threshold

19.13.31 display arp anti-attack configuration

Function

The **display arp anti-attack configuration** command displays the ARP anti-attack configuration.

 Copyright © Huawei Technologies Co., Ltd.

Format

display arp anti-attack configuration { **arp-rate-limit** | **arpmiss-rate-limit** | **arp-speed-limit** | **arpmiss-speed-limit** | **entry-check** | **gateway-duplicate** | **packet-check** | **all** }

Parameters

Parameter	Description	Value
arp-rate-limit	Displays the configuration of rate limit on ARP packets globally or on an interface.	-
arpmiss-rate-limit	Displays the configuration of rate limit on ARP Miss messages.	-
arp-speed-limit	Displays the configuration of rate limit on ARP packets based on the source IP address or source MAC address.	-
arpmiss-speed-limit	Displays the configuration of rate limit on ARP Miss messages based on the source IP address.	-
entry-check	Displays the ARP entry fixing mode.	-
gateway-duplicate	Displays whether gateway anti-collision is enabled.	-
packet-check	Displays whether ARP packet validity check is enabled.	-
all	Displays all ARP anti-attack configurations.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After all ARP anti-attack functions are configured, you can run this command to check all configurations.

Example

Display the maximum rate and rate limiting duration of ARP packets based on the source IP address or source MAC address.

```
<Huawei> display arp anti-attack configuration arp-speed-limit
 ARP speed-limit for source-MAC configuration:
 MAC-address          suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
 0000-0000-0001       150
 Others               200
------------------------------------------------------------------------------
 1 specified MAC addresses are configured, spec is 256 items.

 ARP speed-limit for source-IP configuration:
 IP-address           suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
 10.0.0.20            50
 Others               100
------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 512 items.
```

Display the maximum rate and rate limiting duration of ARP Miss messages based on the source IP address.

```
<Huawei> display arp anti-attack configuration arpmiss-speed-limit
 ARP miss speed-limit for source-IP configuration:
 IP-address           suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
 10.0.0.20            300
 Others               100
------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 128 items.
```

Display the ARP entry fixing mode.

```
<Huawei> display arp anti-attack configuration entry-check
 ARP anti-attack entry-check mode: fixed-mac
```

Display all ARP anti-attack configurations.

```
<Huawei> display arp anti-attack configuration all
 ARP anti-attack packet-check function: enable

 ARP anti-attack entry-check mode: disabled

 ARP gateway-duplicate anti-attack function: disabled

 ARP rate-limit configuration:
------------------------------------------------------------------------------
 Global configuration:
   arp anti-attack rate-limit enable
 Interface configuration:
------------------------------------------------------------------------------

 ARP miss rate-limit configuration:
```

 Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------------
Global configuration:
  arp-miss anti-attack rate-limit enable
------------------------------------------------------------------------------

ARP speed-limit for source-MAC configuration:
MAC-address         suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
0000-0000-0001      200
Others              100
------------------------------------------------------------------------------
1 specified MAC addresses are configured, spec is 256 items.

ARP speed-limit for source-IP configuration:
IP-address          suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
10.0.0.1            512
Others              126
------------------------------------------------------------------------------
1 specified IP addresses are configured, spec is 128 items.

ARP miss speed-limit for source-IP configuration:
IP-address          suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
10.134.23.6         400
Others              500
------------------------------------------------------------------------------
1 specified IP addresses are configured, spec is 128 items.
```

Table 19-142 Description of the display arp anti-attack configuration command output

Item	Description
ARP speed-limit for source-MAC configuration	Rate limit on ARP packets based on the source MAC address. You can run the **19.13.20 arp speed-limit source-mac** command to configure rate limit on ARP packets based on the source MAC address.
ARP speed-limit for source-IP configuration	Rate limit on ARP packets based on the source IP address. You can run the **19.13.21 arp speed-limit source-ip** command to configure rate limit on ARP packets based on the source IP address.
ARP anti-attack packet-check function	Whether MAC address consistency check in an ARP packet is enabled. You can run the **19.13.9 arp anti-attack packet-check sender-mac** command to enable MAC address consistency check in an ARP packet.
ARP miss speed-limit for source-IP configuration	Rate limit on ARP Miss messages based on source IP addresses. You can run the **19.13.29 arp-miss speed-limit source-ip** command to configure rate limit on ARP Miss messages based on the source IP address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ARP anti-attack entry-check mode	ARP entry fixing mode. You can run the **19.13.6 arp anti-attack entry-check enable** command to set the ARP entry fixing mode.
ARP gateway-duplicate anti-attack function:	Whether ARP gateway anti-collision is enabled. You can run the **19.13.7 arp anti-attack gateway-duplicate enable** command to enable ARP gateway anti-collision.
ARP rate-limit configuration	Configuration of rate limit on ARP packets. • **Global configuration** indicates the global configuration of rate limit on ARP packets. • **Interface configuration** indicates the configuration of rate limit on ARP packets on an interface. You can run the **19.13.10 arp anti-attack rate-limit** command to configure rate limit on ARP packets.
ARP miss rate-limit configuration	Configuration of rate limit on ARP Miss messages. **Global configuration** indicates the global configuration of rate limit on ARP Miss messages. You can run the **19.13.25 arp-miss anti-attack rate-limit** command to configure rate limit on ARP Miss messages.
MAC-address	Rate limit on ARP packets based on a specified MAC address. • **ALL** indicates all MAC addresses. • **Others** indicates other MAC addresses except for the specified MAC address.
IP-address	Rate limit on ARP packets and ARP Miss messages based on a specified IP address. • **ALL** indicates all IP addresses. • **Others** indicates other IP addresses except for the specified IP address.
suppress-rate	Rate limit on ARP packets and ARP Miss messages.

Related Topics

19.13.6 arp anti-attack entry-check enable
19.13.7 arp anti-attack gateway-duplicate enable
19.13.21 arp speed-limit source-ip
19.13.29 arp-miss speed-limit source-ip
19.13.9 arp anti-attack packet-check sender-mac
19.13.25 arp-miss anti-attack rate-limit

Copyright © Huawei Technologies Co., Ltd.

19.13.10 arp anti-attack rate-limit

19.13.32 display arp anti-attack gateway-duplicate item

Function

The **display arp anti-attack gateway-duplicate item** command displays ARP gateway anti-collision entries.

Format

display arp anti-attack gateway-duplicate item

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ARP gateway anti-collision is enabled, you can run this command to view ARP anti-collision entries.

Example

Display ARP gateway anti-collision entries.

```
<Huawei> display arp anti-attack gateway-duplicate item
 interface              IP address      MAC address     VLANID   aging time
--------------------------------------------------------------------------------
 Ethernet2/0/0          10.1.1.1        0000-0000-0002  2        150
 Ethernet2/0/1          10.1.1.2        0000-0000-0004  2        170
--------------------------------------------------------------------------------
The number of record(s) in gateway conflict table is 2
```

Table 19-143 Description of the display arp anti-attack gateway-duplicate item command output

Item	Description
interface	Inbound interface of ARP packets.
IP address	IP address of the gateway.
MAC address	Source MAC address of ARP packets.
VLANID	VLAN ID of ARP packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
aging time	Aging time of entries.

Related Topics

19.13.7 arp anti-attack gateway-duplicate enable

19.13.33 display arp flood statistics

Function

The **display arp flood statistics** command displays the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs.

Format

display arp flood statistics

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run this command to view the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs.

Example

Display the statistics on ARP Request packets of all the VLANIF interfaces in a super-VLAN.

```
<Huawei> display arp flood statistics
ARP request packets statistics on supervlan:
Total ARP request packets number :  5100
Sent ARP request packets number :  4000
Dropped ARP request packets number:  1100
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-144 Description of the display arp flood statistics command output

Item	Description
ARP request packets statistics on supervlan	Statistics on ARP Request packets in all super-VLANs.
Total ARP request packets number	Total number of ARP Request packets.
Sent ARP request packets number	Number of sent ARP Request packets.
Dropped ARP request packets number	Number of discarded ARP Request packets when the rate limit on broadcasting ARP Request packets is exceeded on VLANIF interface in all super-VLANs.

Related Topics

19.13.19 arp speed-limit flood-rate

19.13.34 display arp learning strict

Function

The **display arp learning strict** command displays strict ARP learning globally and on all interfaces.

Format

display arp learning strict

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After strict ARP learning is configured, you can run this command to check the configuration.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display strict ARP learning globally and on all interfaces.

```
<Huawei> display arp learning strict
The global configuration:arp learning strict
 Interface                       LearningStrictState
------------------------------------------------------------
 Vlanif100                       force-disable
 Vlanif200                       force-enable
------------------------------------------------------------
 Total:2
 Force-enable:1
 Force-disable:1
```

Table 19-145 Description of the display arp learning strict command output

Item	Description
The global configuration	Global strict ARP learning. The value **arp learning strict** indicates that strict ARP learning has been enabled. If the parameter is left blank, strict ARP learning is disabled. You can run the **19.13.18 arp learning strict (system view)** command to enable strict ARP learning.
Interface	Interface name.
LearningStrictState	Strict ARP learning. • The value **force-enable** indicates that strict ARP learning is enabled. • The value **force-disable** indicates that strict ARP learning is disabled. You can run the **19.13.17 arp learning strict (interface view)** command to enable strict ARP learning.
Total	Total number of interfaces to which strict ARP learning is applied.
Force-enable	Number of the interfaces on which strict ARP learning is enabled.
Force-disable	Number of the interfaces on which strict ARP learning is disabled.

Related Topics

19.13.18 arp learning strict (system view)

19.13.17 arp learning strict (interface view)

19.13.35 display arp packet statistics

Copyright © Huawei Technologies Co., Ltd.

Function

The **display arp packet statistics** command displays the statistics on ARP packets.

Format

display arp packet statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To locate and rectify ARP faults, you can run this command to the statistics on ARP packets.

Example

Display the statistics on ARP packets.

```
<Huawei> display arp packet statistics
ARP Pkt Received:   sum  10088
ARP Learnt Count:   sum     52
ARP Pkt Discard For Limit:   sum      0
ARP Pkt Discard For SpeedLimit:   sum     31
ARP Pkt Discard For Proxy Suppress:   sum    307
ARP Pkt Discard For Other:   sum   9274
```

Table 19-146 Description of the display arp packet statistics command output

Item	Description
ARP Pkt Received	Number of the received ARP packets.
ARP Learnt Count	Times of ARP learning.
ARP Pkt Discard For Limit	Number of ARP packets discarded due to the ARP entry limit.
ARP Pkt Discard For SpeedLimit	Number of ARP packets discarded when the number of ARP packets from a specified source IP address exceeds the limit.
ARP Pkt Discard For Proxy Suppress	Number of packets discarded for the speed limit.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ARP Pkt Discard For Other	Number of the packets discarded due to other causes.

19.13.36 display arp-limit

Function

The **display arp-limit** command displays the maximum number of ARP entries that an interface can dynamically learn.

Format

display arp-limit [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
vlan *vlan-id*	Specifies a VLAN ID. This parameter is available only for Layer 2 interfaces.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the maximum number of ARP entries that an interface can dynamically learn is set, you can run this command to check the configuration.

If **interface** *interface-type interface-number* and **vlan** *vlan-id* are specified, you can view the maximum number of ARP entries that the specified interface can

 Copyright © Huawei Technologies Co., Ltd.

dynamically learn in the specified VLAN. If the two parameters are not specified, the maximum number of ARP entries that each interface can dynamically learn is displayed.

Example

Display the number of ARP entries that each interface can dynamically learn.

```
<Huawei> display arp-limit
 Interface             LimitNum       VlanID         LearnedNum(Mainboard)
------------------------------------------------------------------------------
 Vlanif100             1000           0              0
 Ethernet2/0/0           16384          10               0
------------------------------------------------------------------------------
 Total:2
```

Table 19-147 Description of the display arp-limit command output

Item	Description
Interface	Interface name.
LimitNum	Maximum number of ARP entries that an interface can dynamically learn.
VlanID	ID of the VLAN that the interface belongs to.
LearnedNum(Mainboard)	Number of ARP entries that an interface has learned.

Related Topics

19.13.24 arp-limit

19.13.37 reset arp anti-attack statistics check user-bind

Function

The **reset arp anti-attack statistics check user-bind** command clears the statistics on discarded ARP packets matching no binding entry.

Format

reset arp anti-attack statistics check user-bind interface *interface-type interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. Where, • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After DAI is enabled and some ARP packets matching no binding entry are discarded, you can run this command to clear the statistics on the discarded ARP packets.

Example

Clear the statistics on discarded ARP packets on Eth2/0/0.

```
<Huawei> reset arp anti-attack statistics check user-bind interface ethernet 2/0/0
```

Related Topics

19.13.5 arp anti-attack check user-bind enable

19.13.38 reset arp anti-attack statistics rate-limit

Function

The **reset arp anti-attack statistics rate-limit** command clears the statistics on ARP packets discarded when the rate of ARP packets exceeds the limit.

Format

reset arp anti-attack statistics rate-limit { **global** | **interface** *interface-type interface-number* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
global	Indicates that statistics on discarded ARP packets are cleared globally.	-
interface *interface-type interface-number*	Specifies the interface type and number. Where, • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After rate limit on ARP packets is enabled, the device discards the excess packets when the rate of ARP packets exceeds the limit. You can run this command to clear the statistics on the discarded ARP packets.

Example

Clear the statistics on ARP packets discarded when the rate of ARP packets exceeds the limit globally.

```
<Huawei> reset arp anti-attack statistics rate-limit global
```

Related Topics

19.13.13 arp anti-attack rate-limit enable

19.13.39 reset arp flood statistics

Function

The **reset arp flood statistics** command clears the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs.

Format

reset arp flood statistics

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After this command is run, the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs are cleared and cannot be restored.

Example

Clear the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs is cleared.

```
<Huawei> reset arp flood statistics
```

Related Topics

19.13.19 arp speed-limit flood-rate

19.13.40 reset arp packet statistics

Function

The **reset arp packet statistics** command clears the statistics on ARP packets.

Format

reset arp packet statistics

Parameters

None

Views

User view

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display arp packet statistics** command to display the statistics on ARP packets. To obtain correct statistics, run the **reset arp packet statistics** command to clear existing statistics first.

The **reset arp packet statistics** command clears the ARP packet statistics only on the main control board.

Example

Clear the statistics on all ARP packets.

```
<Huawei> reset arp packet statistics
```

19.14 DHCP Snooping Configuration Commands

NOTE

- The 4GE-2S, 4ES2GP-S, 4ES2G-S, and 9ES2 cards do not support DHCP snooping.
- AR100&AR120&AR150&AR160&AR200&AR1200 series do not support DHCPv6 snooping.
- The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the following commands:
  - **19.14.14 dhcp snooping trusted**
  - **19.14.16 dhcp snooping user-bind autosave**
  - **8.9.9 dhcpv6 interface-id format**
  - **19.14.19 dhcpv6 option18 format**
  - **19.14.20 dhcpv6 option37 format**
  - **19.14.21 dhcpv6 { option18 | option37 } enable**
  - **19.14.22 dhcpv6 snooping relay-information enable**
  - **19.14.28 display dhcpv6 snooping user-bind**

19.14.1 arp dhcp-snooping-detect enable

Function

The **arp dhcp-snooping-detect enable** command enables association between the Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) snooping.

The **undo arp dhcp-snooping-detect enable** command disables association between ARP and DHCP snooping.

By default, association between ARP and DHCP snooping is disabled.

Format

arp dhcp-snooping-detect enable

undo arp dhcp-snooping-detect enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DHCP client sends a DHCP Release message to release its IP address, the DHCP snooping-enabled device immediately deletes the binding entry of the DHCP client. If a DHCP client is abnormally disconnected and cannot send a DHCP Release message, the DHCP snooping-enabled device cannot immediately delete the binding entry of the DHCP client.

If association between ARP and DHCP snooping is enabled using this command and no ARP entry corresponding to the IP address in the DHCP snooping binding entry is found, the DHCP snooping-enabled device performs an ARP probe on the IP address. If no user is detected for consecutive four times, the DHCP snooping-enabled device deletes the DHCP snooping binding entry corresponding to the IP address. (The probe interval is 20 seconds, and the probe times and probe interval are fixed values and cannot be modified.) If the DHCP snooping-enabled device supports the DHCP relay function, this device then sends a DHCP Release message in place of the DHCP client to notify the DHCP server to release the IP address.

Prerequisites

Before association between the ARP and DHCP snooping is enabled, ensure that an IP address configured on the device is on the same network segment as the IP address of the client for ARP probe.

Example

Enable association between ARP and DHCP snooping on the device.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] arp dhcp-snooping-detect enable
```

Related Topics

19.14.11 dhcp snooping enable

8.2.2 arp detect-times

19.14.2 dhcp option82 enable

 Copyright © Huawei Technologies Co., Ltd.

Function

The **dhcp option82 enable** command enables a device to insert the Option 82 field to a DHCP message.

The **undo dhcp option82 enable** command disables a device from inserting the Option 82 field to a DHCP message.

By default, a device does not insert the Option 82 field to a DHCP message.

Format

dhcp option82 { **insert** | **rebuild** } **enable**

undo dhcp option82 { **insert** | **rebuild** } **enable**

Parameters

Parameter	Description	Value
insert	Enables a device to insert the Option 82 field to a DHCP message.	-
rebuild	Enables a device to forcibly insert the Option 82 field to a DHCP message.	-

Views

VLAN view, Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security.

The device inserts the Option 82 field to a DHCP message in two modes:

- Insert mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device checks whether the Option 82 field contains the remote ID. If so, the device retains the Option 82 field; if not, the device inserts the remote ID.
- Rebuild mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device deletes the original Option 82 field and inserts the Option 82 field set by the administrator.

 Copyright © Huawei Technologies Co., Ltd.

The device handles the reply packets from the DHCP server in the same way regardless of whether the Insert or Rebuild method is used.

- The DHCP reply packets contain Option 82:
  - If the DHCP request packets received by the device do not contain Option 82, the device deletes Option 82 from the DHCP reply packets, and forwards the packets to the DHCP client.
  - If the DHCP request packets contain Option 82, the device changes the Option 82 format in the DHCP reply packets into the Option 82 format in the DHCP request packets, and forwards the packets to the DHCP client.
- If the DHCP reply packets do not contain Option 82, the device directly forwards the packets.

NOTE

The physical interface can insert Option82 to the DHCP packets directly forwarded, but does not insert Option82 to the DHCP packets forwarded through a tunnel.

Prerequisites

DHCP snooping has been enabled on the device, or the device has been configured as a DHCP relay agent.

Precautions

- When receiving a DHCP Request message, the device checks whether the field GIADDR in the packet is 0. If so, the **dhcp option82 enable** command takes effect; if not, this command does not take effect.
- DHCP Option 82 must be configured on the user-side of a device; otherwise, the DHCP messages sent to the DHCP server will not carry Option 82.

Example

Enable the device to insert the Option 82 field to DHCP messages on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 insert enable
```

Enable the device to forcibly insert the Option 82 field to DHCP messages in VLAN 100.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] dhcp option82 rebuild enable
```

Related Topics

8.3.28 dhcp select relay
19.14.11 dhcp snooping enable
19.14.23 display dhcp option82 configuration

19.14.3 dhcp option82 format

Function

The **dhcp option82 format** command configures the format of the Option 82 field in a DHCP message.

 Copyright © Huawei Technologies Co., Ltd.

The **undo dhcp option82 format** command restores the default format of the Option 82 field in a DHCP message.

By default, the Option 82 field in a DHCP message is in the format of **default**.

Format

dhcp option82 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format** { **default** | **common** | **extend** | **user-defined** *text* }

undo dhcp option82 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format**

Parameters

Parameter	Description	Value
circuit-id	Indicates the circuit ID (CID) in the Option 82 field. If the CID is not specified, the format of the Option 82 field is **default**.	-
remote-id	Indicates the remote ID (RID) in the Option 82 field. If the RID is not specified, the format of the Option 82 field is **default**.	-
default	Indicates the default format of the Option 82 field. • CID format: interface name:svlan.cvlan host name/0/0/0/0/0, in ASCII format • RID format: device MAC address, in hexadecimal notation	-
common	Indicates the common format of the Option 82 field. • CID format: {eth|trunk}slot ID/subcard ID/port ID:svlan.cvlan host name0/0/0/0/0, in ASCII format • RID format: device MAC address (6 bytes), in ASCII format	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
extend	Indicates the extended format of the Option 82 field. • CID format: circuit-id type (0) + length (4) + S-VLAN ID (2 bytes) + slot ID (5 bits) + subslot ID (3 bits) + port (1 byte), in hexadecimal notation • RID format: remote-id type (0) + length (6) + device MAC address (6 bytes), in hexadecimal notation In the CID and RID formats, the values without a unit are fixed values of the fields; the values with a unit indicate the field lengths.	-
user-defined *text*	Indicates the user-defined format of the Option 82 field.	The value is a string of 1 to 255 characters. For details, see the description in "Usage Guideline."
vlan *vlan-id*	Indicates an outer VLAN ID. If a VLAN ID is specified, only the format of the Option 82 field in the DHCP messages sent from the specified VLAN is configured. If no VLAN is specified, the format of the Option 82 field in all the DHCP messages received by the interface is configured.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Indicates an inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

System view, Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of inserting the Option 82 field to DHCP messages is enabled, you can use the **dhcp option82 format** command to configure the format of the Option 82 field.

 Copyright © Huawei Technologies Co., Ltd.

If you run the **dhcp option82 format** command in the system view, the command takes effect for all the DHCP messages on all the interfaces of the device.

You can use the following keywords to define the Option 82 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, Eth2/0/0. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.

 Copyright © Huawei Technologies Co., Ltd.

- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 82 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- The contents in quotation marks (" ") are encapsulated in a character string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
  - A hexadecimal notation string can contain numerals, spaces, and % + keywords.
  - In a hexadecimal notation string, numbers are encapsulated in the Option 82 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
  - All the spaces in a hexadecimal character string are ignored.
  - By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
  - If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
  - A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
  - If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
  - A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- All Option82 fields configured in the system view or in the same interface view share a length of 1-255 bytes. If their total length exceeds 255 bytes, some Option82 information will be lost.
- There is no limit on the number of Option 82 fields configured on the device. However, a large number of Option 82 fields will occupy a lot of memory and prolong the device processing time. To ensure device performance, you are advised to configure Option 82 fields based on the service requirements and device memory size.

Example

Configure the default format for the CID in the Option 82 field.

```
<Huawei> system-view
[Huawei] dhcp option82 circuit-id format default
```

Configure the extended format for the CID and RID in the Option 82 field.

```
<Huawei> system-view
[Huawei] dhcp option82 format extend
```

Configure the user-defined string for the CID in the Option 82 field and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<Huawei> system-view
[Huawei] dhcp option82 circuit-id format user-defined "%portname:%svlan.%cvlan %sysname"
```

Configure a hexadecimal notation string for the CID of the Option 82 field and encapsulate the CID type (fixed as 0, indicating the hexadecimal notation), length (excluding the lengths of the CID type and the keyword length itself), outer VLAN ID, slot ID (5 bits), subcard ID (3 bits), and port ID (8 bits).

```
<Huawei> system-view
[Huawei] dhcp option82 circuit-id format user-defined 0 %length %svlan %5slot %3subslot %8port
```

Configure the user-defined string for the RID in the Option 82 field and encapsulate the device MAC address in hexadecimal notation.

```
<Huawei> system-view
[Huawei] dhcp option82 remote-id format user-defined %mac
```

On Eth2/0/0, configure the default format for the CID in the Option 82 field.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 circuit-id format default
```

On Eth2/0/0, configure the extended format for the CID and RID in the Option 82 field of DHCP messages from VLAN 10.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 vlan 10 format extend
```

On Eth2/0/0, configure a user-defined format for the CID in the Option 82 field and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 circuit-id format user-defined "%portname:%svlan.%cvlan
%sysname"
```

 Copyright © Huawei Technologies Co., Ltd.

On Eth2/0/0, configure a hexadecimal notation string for the CID of the Option 82 field and encapsulate the CID type (fixed as 0, indicating the hexadecimal notation), length (excluding the lengths of the CID type and the keyword length itself), outer VLAN ID, slot ID (5 bits), subcard ID (3 bits), and port ID (8 bits).

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 circuit-id format user-defined 0 %length %svlan %5slot %3subslot %8port
```

On Eth2/0/0, configure the user-defined format for the RID in the Option 82 field and encapsulate the device MAC address in hexadecimal notation.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 remote-id format user-defined %mac
```

Related Topics

19.14.2 dhcp option82 enable

19.14.4 dhcp server detect

Function

The **dhcp server detect** command enables detection of DHCP servers.

The **undo dhcp server detect** command disables detection of DHCP servers.

By default, detection of DHCP servers is disabled.

Format

dhcp server detect

undo dhcp server detect

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If bogus DHCP servers exist on the network, they send incorrect information to DHCP clients, such as the incorrect gateway address, incorrect DNS server, and incorrect IP address. As a result, DHCP clients cannot access the network or access incorrect networks.

 Copyright © Huawei Technologies Co., Ltd.

After detection of DHCP servers is enabled, a DHCP snooping device checks and stores all information about DHCP servers in the DHCP Reply messages, such as DHCP server address and DHCP client port number, in the log. Based on logs, the network administrator checks for bogus DHCP servers on the network to maintain the network.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

Enable detection of DHCP servers.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] dhcp server detect
```

Related Topics

19.14.11 dhcp snooping enable

19.14.5 dhcp snooping alarm enable

Function

The **dhcp snooping alarm enable** command enables alarm for discarded DHCP messages.

The **undo dhcp snooping alarm enable** command disables alarm for discarded DHCP messages.

By default, the alarm function for discarded DHCP messages is disabled.

Format

dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } **enable** [**threshold** *threshold*]

undo dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } **enable** [**threshold**]

Parameters

Parameter	Description	Value
user-bind	Generates an alarm when the number of DHCPv4 Request messages discarded because they do not match DHCP snooping binding entries reaches the threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mac-address	Generates an alarm when the number of DHCPv4 request messages discarded because the CHADDR field in the DHCP messages does not match the source MAC address in the data frame header reaches the threshold.	-
untrust-reply	Generates an alarm when the number of DHCPv4 Response messages discarded by untrusted interfaces reaches the threshold.	-
threshold *threshold*	Specifies the alarm threshold. When the number of discarded DHCPv4 messages reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000.

Views

Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function is enabled, alarm messages are displayed if DHCP attacks occur and the number of discarded attack messages reaches the threshold. The minimum interval for sending alarm messages is 1 minute. You can run the **19.14.6 dhcp snooping alarm threshold** command to set the alarm threshold.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

By default, a device does not check messages received by the clients. Therefore, to make the command take effect, ensure the following is ready:

- The device has been enabled to check DHCP messages against the binding entries using the **19.14.9 dhcp snooping check user-bind enable** command before the **dhcp snooping alarm user-bind enable** command is run.
- The device has been enabled to check whether the CHADDR field is the same as the source MAC address in the header of a DHCPv4 Request message using the **19.14.8 dhcp snooping check mac-address enable** command before the **dhcp snooping alarm mac-address enable** command is run.

To ensure that alarms can be properly reported, you need to run the **8.3.106 snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP

 Copyright © Huawei Technologies Co., Ltd.

module is enabled to report the corresponding alarm using the **8.3.73 display snmp-agent trap feature-name dhcp all** command.

Example

On Eth2/0/0, enable DHCP snooping, enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address in the Ethernet frame header, and enable alarm for the DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping check mac-address enable
[Huawei-Ethernet2/0/0] dhcp snooping alarm mac-address enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.6 dhcp snooping alarm threshold

19.14.6 dhcp snooping alarm threshold

Function

The **dhcp snooping alarm threshold** command sets the alarm threshold for the number of DHCP messages discarded by DHCP snooping.

The **undo dhcp snooping alarm threshold** command restores the default alarm threshold.

By default, an alarm is generated in the system when at least 100 DHCP snooping messages are discarded, and the alarm threshold on an interface is set using the **dhcp snooping alarm threshold** command in the system view.

Format

In the system view:

dhcp snooping alarm threshold *threshold*

undo dhcp snooping alarm threshold

In the interface view:

dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } **threshold** *threshold*

undo dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } **threshold**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the number of DHCP snooping-discarded messages.	The value is an integer that ranges from 1 to 1000.
user-bind	Specifies the alarm threshold for the number of DHCPv4 Request messages discarded because they do not match the DHCP snooping binding entries.	-
mac-address	Specifies the alarm threshold for the number of DHCP messages discarded because the CHADDR field in the DHCPv4 request messages does not match the source MAC address in the data frame header.	-
untrust-reply	Specifies the alarm threshold for the number of DHCPv4 Response messages discarded by untrusted interfaces.	-

Views

System view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After trap for discarded DHCP messages is enabled, run the **dhcp snooping alarm threshold** command to specify the alarm threshold for the number of DHCP messages discarded by DHCP snooping. If the alarm threshold is not set on an interface, the interface uses the global alarm threshold.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

The DHCP snooping alarm function has been enabled using the **dhcp snooping alarm** { **user-bind** | **mac-address** | **untrust-reply** } **enable** command.

Precautions

If you run the **dhcp snooping alarm threshold** command in the system view, the command takes effect on all the interfaces of the device.

 Copyright © Huawei Technologies Co., Ltd.

If you specify an alarm threshold for the number of DHCP messages discarded by DHCP snooping in the system view, an alarm is generated when the number of all the discarded DHCP messages reaches the threshold.

Example

Set the global alarm threshold for the number of discarded DHCP messages to 200.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] dhcp snooping alarm threshold 200
```

On Eth2/0/0, enable DHCP snooping, enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address in the Ethernet frame header, and enable alarm for the DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address. Set the alarm threshold to 1000.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping check mac-address enable
[Huawei-Ethernet2/0/0] dhcp snooping alarm mac-address enable
[Huawei-Ethernet2/0/0] dhcp snooping alarm mac-address threshold 1000
```

19.14.7 dhcp snooping check dhcp-giaddr enable

Function

The **dhcp snooping check dhcp-giaddr enable** command enables the device to check whether the GIADDR field in DHCP messages is 0.

The **undo dhcp snooping check dhcp-giaddr enable** command disables the device from checking whether the GIADDR field in DHCP messages is 0.

By default, the device does not check whether the GIADDR field in DHCP messages is 0.

Format

dhcp snooping check dhcp-giaddr enable

undo dhcp snooping check dhcp-giaddr enable

Parameters

None

Views

VLAN view, Interface view, Port group view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that the device obtains parameters such as MAC addresses for generating a binding table, DHCP snooping needs to be applied to Layer 2 access devices or the first DHCP relay agent from the device. Therefore, the GIADDR field in the DHCP messages received by the DHCP snooping-enabled device is 0. If the GIADDR field is not 0, the message is unauthorized and then discarded.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check dhcp-giaddr enable** command in the VLAN view, the command takes effect on all the DHCP messages from the specified VLAN. If you run the **dhcp snooping check dhcp-giaddr enable** command in the interface view, the command takes effect on all the DHCP messages received by the specified interface.

Example

Enable the device to check whether the GIADDR field in DHCP messages from VLAN1 10 is 0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcp snooping check dhcp-giaddr enable
```

Enable the device to check whether the GIADDR field in DHCP messages received on Eth2/0/0 is 0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping check dhcp-giaddr enable
```

Related Topics

8.3.18 dhcp enable

19.14.11 dhcp snooping enable

 Copyright © Huawei Technologies Co., Ltd.

19.14.8 dhcp snooping check mac-address enable

Function

The **dhcp snooping check mac-address enable** command enables the device to check whether the CHADDR field matches the source MAC address in the header of a DHCP Request message.

The **undo dhcp snooping check mac-address enable** command disables the device from checking whether the CHADDR field matches the source MAC address in the header of a DHCP Request message.

By default, the device does not check whether the CHADDR field is the same as the source MAC address in the header of a DHCP Request message.

Format

dhcp snooping check mac-address enable

undo dhcp snooping check mac-address enable

Parameters

None

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In normal situations, the CHADDR field in a DHCP Request message matches the MAC address of the DHCP client that sends the message. The DHCP server identifies the client MAC address based on the CHADDR field in the DHCP Request message. If attackers continuously apply for IP addresses by changing the CHADDR field in the DHCP Request message, addresses in the address pool on the DHCP server may be exhausted. As a result, authorized users cannot obtain IP addresses.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check mac-address enable** command in the VLAN view, the command takes effect on all the DHCP messages in the specified VLAN received by all the interfaces on the device. If you run the **dhcp snooping check**

 Copyright © Huawei Technologies Co., Ltd.

mac-address enable command in the interface view, the command takes effect for all the DHCP messages received on the interface.

Example

Enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address on Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping check mac-address enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.9 dhcp snooping check user-bind enable

19.14.9 dhcp snooping check user-bind enable

Function

The **dhcp snooping check user-bind enable** enables the device to check DHCP messages against the DHCP snooping binding table.

The **undo dhcp snooping check user-bind enable** disables the device from checking DHCP messages against the DHCP snooping binding table.

By default, the device does not check DHCP messages against the DHCP snooping binding table.

Format

dhcp snooping check user-bind enable

undo dhcp snooping check user-bind enable

Parameters

None

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DHCP snooping binding table is generated, the device checks DHCP Request and Release messages against the binding table. The device forwards only

 Copyright © Huawei Technologies Co., Ltd.

DHCP messages that match binding entries. This prevents unauthorized users from sending bogus DHCP Request or Release messages to extend or release IP addresses.

The matching rules are as follows:

- When the device receives a DHCP Request message, it performs the following operations:
  a. Checks whether the destination MAC address is all Fs. If so, the device considers the user to have gone online for the first time and directly forwards the message. If not, the device considers the user to have sent the DHCP Request message to renew the IP address lease and checks the DHCP Request message against the DHCP snooping binding table.
  b. Checks whether the CHADDR field in the DHCP Request message matches a DHCP snooping binding entry. If not, the device considers the user to have gone online for the first time and directly forwards the message. If so, the device checks whether the VLAN ID, IP address, and interface number of the message match DHCP snooping binding entries. If all these fields match a DHCP snooping binding entry, the device forwards the message; otherwise, the device discards the message.
- When receiving a DHCP Release message, the device checks whether the VLAN ID, IP address, MAC address, and interface number of the message match a dynamic DHCP snooping binding entry. If so, the device forwards the message; otherwise, the device discards the message.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check user-bind enable** command in the VLAN view, the command takes effect for all the DHCP messages received from the specified VLAN. If you run the **dhcp snooping check user-bind enable** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

Example

Enable the device to check DHCP messages against the DHCP snooping binding table in VLAN 10.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcp snooping enable
[Huawei-vlan10] dhcp snooping check user-bind enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.8 dhcp snooping check mac-address enable

 Copyright © Huawei Technologies Co., Ltd.

19.14.10 dhcp snooping disable

Function

The **dhcp snooping disable** command disables DHCP snooping on an interface.

The **undo dhcp snooping disable** command cancels the configuration.

By default, if the **19.14.11 dhcp snooping enable** command is used on an interface or in a VLAN that an interface belongs to, DHCP snooping is enabled on this interface.

Format

dhcp snooping disable

undo dhcp snooping disable

Parameters

None

Views

Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you run the **dhcp snooping enable** command to enable DHCP snooping in a VLAN, DHCP snooping is enabled on all the interfaces in the VLAN. If you do not run the **dhcp snooping enable** command to enable DHCP snooping on an interface, you cannot run the **undo dhcp snooping enable** command to disable DHCP snooping on the interface. To address this problem, run the **dhcp snooping disable** command to disable DHCP snooping on the interface. Users can properly go online from this interface, but no dynamic binding entry is generated.

Precautions

- The **dhcp snooping disable** command does not only disable DHCP snooping on an interface, but also clears the DHCP snooping configuration and the dynamic binding table. The **undo dhcp snooping enable** command, however, only disables DHCP snooping on the interface and does not clear the configuration or the dynamic binding table.
- The **undo dhcp snooping disable** command enables DHCP snooping on an interface. To enable DHCP snooping, run the **dhcp snooping enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable DHCP snooping on Eth2/0/0 in VLAN 10.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcp snooping enable
[Huawei-vlan10] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping disable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.11 dhcp snooping enable

Function

The **dhcp snooping enable** command enables DHCP snooping.

The **undo dhcp snooping enable** command disables DHCP snooping.

By default, DHCP snooping is disabled on the device.

Format

In the system view:

dhcp snooping enable [**ipv4** | **ipv6** | **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping enable [**ipv4** | **ipv6** | **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the VLAN view and interface view:

dhcp snooping enable

undo dhcp snooping enable

Parameters

Parameter	Description	Value
ipv4	Indicates that the device processes only DHCPv4 messages. **NOTE** The AR169RW-P-M9 does not support this parameter.	-
ipv6	Indicates that the device processes only DHCPv6 messages. **NOTE** The AR169RW-P-M9 does not support this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables DHCP snooping in a specified VLAN. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The specified VLAN ID must exist.

Views

System view, VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DHCP snooping is a security function to protect DHCP. When you run the **dhcp snooping enable** command to enable DHCP snooping on a device, the device can process both DHCPv4 and DHCPv6 messages. In practice, however, if the DHCP snooping device needs to process only DHCPv4 or DHCPv6 messages, you can run the **dhcp snooping enable ipv4** or **dhcp snooping enable ipv6** command, which improves CPU efficiency.

You must enable DHCP snooping in the system view before enabling DHCP snooping on an interface or in a VLAN.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Follow-up Procedure

Run the **dhcp snooping trusted** command to configure the interface connected to the DHCP server as a trusted interface. A binding table is generated.

Precautions

The **dhcp snooping enable** command in the system view is the prerequisite for DHCP snooping-related functions. After the **undo dhcp snooping enable** command is run, all DHCP snooping-related configurations of the device are deleted. After DHCP snooping is enabled again using the **dhcp snooping enable** command, all DHCP snooping-related configurations of the device are restored to the default configurations.

If you run the **dhcp snooping enable** command in the VLAN view, the command takes effect for all the DHCP messages from the specified VLAN. If you run the **dhcp snooping enable** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable DHCP snooping globally and configure the device to process only ipv4 messages.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable ipv4
```

Enable DHCP snooping on Eth 2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
```

Enable DHCP snooping in VLAN 100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 100
[Huawei-vlan100] dhcp snooping enable
```

Enable DHCP snooping in VLANs ranging from VLAN 20 to VLAN 25 in a batch.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan batch 20 to 25
[Huawei] dhcp snooping enable vlan 20 to 25
```

19.14.12 dhcp snooping enable no-user-binding

Function

The **dhcp snooping enable no-user-binding** command disables the interfaces from generating DHCP snooping binding entries after DHCP snooping is enabled.

The **undo dhcp snooping enable no-user-binding** command restores the default setting.

By default, an interface generates DHCP snooping binding entries after DHCP snooping is enabled.

Format

System view:

dhcp snooping enable no-user-binding vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping enable no-user-binding vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

VLAN view, interface view:

dhcp snooping enable no-user-binding

undo dhcp snooping enable no-user-binding

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Disables the interfaces in the specified VLANs from generating DHCP snooping binding entries. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

After DHCP snooping is enabled on a device, the device generates DHCP snooping binding entries for users by default. If the number of binding entries on the device reaches the upper limit, new users cannot go online. In certain scenarios, for example, on a trusted DHCP network, if you do not want to limit the number of online users but want to record user location information, run the **dhcp snooping enable no-user-binding** command to disable the device from generating DHCP snooping binding entries.

When the command is executed in an interface view, the command takes effect for all DHCP users connecting to the interface. When the command is executed in the VLAN view, the command takes effect for all the DHCP users belonging to this VLAN on all interfaces. When the command is executed in the system view, the command takes effect in the same way as it is executed in the VLAN view, except that multiple VLANs can be specified.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

After this command is executed, the device deletes the binding entries from the corresponding VLAN or interface.

If the DHCP snooping binding entry-dependent function such as IPSG or DAI is configured on the device, the corresponding function does not take effect after this command is run.

This command cannot be used together with **19.14.9 dhcp snooping check user-bind enable**; otherwise, online users cannot go offline.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the system view, disable the interfaces in VLAN 10 and VLAN 20 from generating DHCP snooping binding entries.

```
<Huawei> system-view
[Huawei] dhcp snooping enable no-user-binding vlan 10 20
```

In the VLAN view, disable the interfaces in VLAN 10 from generating DHCP snooping binding entries.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] dhcp snooping enable no-user-binding
```

In the interface view, disable Eth2/0/0 from generating DHCP snooping binding entries.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable no-user-binding
```

Related Topics

19.14.11 dhcp snooping enable

19.14.22 dhcpv6 snooping relay-information enable

19.14.13 dhcp snooping max-user-number

Function

The **dhcp snooping max-user-number** command sets the maximum number of DHCP snooping binding entries to be learned on an interface.

The **undo dhcp snooping max-user-number** command restores the default maximum number of DHCP snooping binding entries to be learned on an interface.

By default, the number of learned DHCP snooping binding entries is the maximum number of DHCP snooping binding entries that can be learned by the entire device.

Format

dhcp snooping max-user-number *max-user-number*

undo dhcp snooping max-user-number

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of DHCP snooping binding entries that can be learned on an interface.	The value is an integer that varies depending on product models.

 Copyright © Huawei Technologies Co., Ltd.

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp snooping max-user-number** command sets the maximum number of DHCP snooping binding entries to be learned on an interface. If the number of DHCP snooping binding entries reaches the maximum value, subsequent users cannot access.

If you run the **dhcp snooping max-user-number** command in the VLAN view, the command takes effect on all the interfaces in the VLAN. If you run the **dhcp snooping max-user-number** command in the VLAN view, and the interface view, the smallest value takes effect.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

Set the maximum number of DHCP users to 100 on Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping max-user-number 100
```

Set the maximum number of DHCP users in VLAN 100 to 100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 100
[Huawei-vlan100] dhcp snooping enable
[Huawei-vlan100] dhcp snooping max-user-number 100
```

Related Topics

19.14.11 dhcp snooping enable

19.14.24 display dhcp snooping

19.14.14 dhcp snooping trusted

Function

The **dhcp snooping trusted** command configures an interface as a trusted interface.

 Copyright © Huawei Technologies Co., Ltd.

The **undo dhcp snooping trusted** command configures an interface as an untrusted interface.

By default, an interface is an untrusted interface.

NOTE

AR1200 series routers do not support this command.

Format

In the VLAN view:

dhcp snooping trusted interface *interface-type interface-number*

undo dhcp snooping trusted interface *interface-type interface-number*

In the interface view:

dhcp snooping trusted

undo dhcp snooping trusted

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface in a VLAN. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable DHCP clients to obtain IP addresses from authorized DHCP servers, DHCP snooping supports the trusted interface and untrusted interfaces. The trusted interface forwards DHCP messages while untrusted interfaces discard received DHCP ACK messages and DHCP Offer messages.

An interface directly or indirectly connected to the DHCP server trusted by the administrator needs to be configured as the trusted interface, and other interfaces are configured as untrusted interfaces. This ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

In the system view, run the **dhcp snooping enable** command to enable DHCP snooping.

Precautions

If you run the **dhcp snooping trusted** command in the VLAN view, the command takes effect for all the DHCP messages received from the specified VLAN. If you run the **dhcp snooping trusted** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

Example

Configure Eth2/0/0 in VLAN 100 as the trusted interface.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 100
[Huawei-vlan100] dhcp snooping trusted interface ethernet 2/0/0
```

Configure Eth2/0/0 as the trusted interface.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping trusted
```

Related Topics

19.14.11 dhcp snooping enable

19.14.15 dhcp snooping user-alarm percentage

Function

The **dhcp snooping user-alarm percentage** command configures the alarm thresholds for the percentage of DHCP snooping binding entries.

The **undo dhcp snooping user-alarm percentage** command restores the default alarm thresholds for the percentage of DHCP snooping binding entries.

By default, the lower alarm threshold for the percentage of DHCP snooping binding entries is 50, and the upper alarm threshold for the percentage of DHCP snooping binding entries is 100.

Format

dhcp snooping user-alarm percentage *percent-lower-value percent-upper-value*

undo dhcp snooping user-alarm percentage

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of DHCP snooping binding entries.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of DHCP snooping binding entries.	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 you run the **19.14.13 dhcp snooping max-user-number** command to set the maximum number of DHCP snooping binding entries on an interface, you can run the **dhcp snooping user-alarm percentage** command to set the alarm thresholds for the percentage of DHCP snooping binding entries.

When the percentage of learned DHCP snooping binding entries against the maximum number of DHCP snooping entries allowed by the device reaches or exceeds the upper alarm threshold, the device generates an alarm. When the percentage of learned DHCP snooping binding entries against the maximum number of DHCP snooping entries allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm.

Example

Set the lower alarm threshold for the DHCP user count percentage to 30 and the upper alarm threshold to 80.

```
<Huawei> system-view
[Huawei] dhcp snooping user-alarm percentage 30 80
```

Related Topics

19.14.13 dhcp snooping max-user-number

19.14.16 dhcp snooping user-bind autosave

Copyright © Huawei Technologies Co., Ltd.

Function

The **dhcp snooping user-bind autosave** command enables automatic backup of the DHCP snooping binding table.

The **undo dhcp snooping user-bind autosave** command disables automatic backup of the DHCP snooping binding table.

By default, automatic backup of the DHCP snooping binding table is disabled.

Format

dhcp snooping user-bind autosave *file-name* [**write-delay** *delay-time*]

undo dhcp snooping user-bind autosave

Parameters

Parameter	Description	Value
file-name	Specifies the path for storing the file that backs up the binding table and the file name. The file path and name supported by the device must be both entered.	The value is a string of 1 to 51 case-insensitive characters without spaces.
write-delay *delay-time*	Specifies the interval for local automatic backup of the DHCP snooping binding table. If this parameter is not specified, the backup interval is the default value.	The value is an integer that ranges from 60 to 4294967295, in seconds. By default, the interval for local automatic backup of the DHCP snooping binding table is 86400 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp snooping user-bind autosave** command can retain the configured DHCP snooping binding entries after the device restarts. After a DHCP snooping binding table is generated, you can run the **dhcp snooping user-bind autosave** command to enable automatic backup of the DHCP snooping binding table.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

This prevents data loss in the DHCP snooping binding table. The suffix of the file must be .tbl.

Currently, the DHCP snooping binding table can be backed up to only the SD card.

If the system restarts within one day after the system time is changed, immediately run the **dhcp snooping user-bind autosave** command again to back up the latest dynamic binding entries because it is not the time to update the binding table. If you do not run this command, the lease will be inconsistent with the current system time after the dynamic binding table is restored.

Example

Configure the device to back up the DHCP snooping binding table to the file **backup.tbl** in the SD card every 5000 seconds.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] dhcp snooping user-bind autosave sd1:/backup.tbl write-delay 5000
```

Related Topics

19.14.11 dhcp snooping enable

19.14.17 dhcp snooping user-transfer enable

Function

The **dhcp snooping user-transfer enable** command enables location transition for DHCP snooping users.

The **undo dhcp snooping user-transfer enable** command disables location transition for DHCP snooping users.

By default, location transition is enabled for DHCP snooping users.

Format

dhcp snooping user-transfer enable

undo dhcp snooping user-transfer enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In mobile applications, if a user goes online from interfaceA and then switches to interfaceB, you need to enable location transition for DHCP snooping users.

Prerequisites

DHCP snooping has been enabled on the device using the **19.14.11 dhcp snooping enable** command.

Example

Disable location transition for DHCP snooping users.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] undo dhcp snooping user-transfer enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.18 dhcpv6 interface-id format

Function

The **dhcpv6 interface-id format** command configures the Interface-ID format in DHCPv6 packets.

The **undo dhcpv6 interface-id format** command restores the default Interface-ID format in DHCPv6 packets.

By default, the Interface-ID format in DHCPv6 packets is **default**.

Format

dhcpv6 interface-id format { **default** | **user-defined** *text* }

undo dhcpv6 interface-id format

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
default	Specifies the default Interface-ID format. The default Interface-ID format is %04svlan.%04cvlan.%mac:%portname. The values of the S-VLAN and C-VLAN are integers containing four characters. If the length is fewer than four characters, the value is prefixed with 0s. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is VLANIF100, and the device MAC address is 6afe-870b-0000, the Interface-ID generated during the system parsing process is 0011.0022.6afe870b0000:vlanif100.	-
user-defined *text*	Specifies a user-defined format as the Interface-ID format. A user-defined format can be: • Format defined by keywords: The Interface-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Interface-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 19-148**. • Format defined by common character strings: The Interface-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Interface-ID can be directly defined as N8. • Mixed format: The Interface-ID is defined by both the keywords and common character strings. For example, the Interface-ID can be defined as %sysname N8.	The value is a string of case-sensitive characters without spaces. The character string contains 1 to 251 characters, excluding the quotation marks.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The Interface-ID records user access information such as the inbound interfaces of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Interface-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 interface-id format** command to configure the format of the Interface-ID inserted into DHCPv6 packets.

Table 19-148 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.

 Copyright © Huawei Technologies Co., Ltd.

Keyword	Description
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

- The user-defined format content must be specified between the double quotation marks (""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.
- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Configure a user-defined format as the format of the Interface-ID in DHCPv6 packets and the device MAC address as the encapsulated content.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 interface-id format user-defined "%mac"
```

19.14.19 dhcpv6 option18 format

Function

The **dhcpv6 option18 format** command configures the format of the Option 18 field in a DHCPv6 message.

The **undo dhcpv6 option18 format** command restores the default format of the Option 18 field in a DHCPv6 message.

 Copyright © Huawei Technologies Co., Ltd.

By default, the format of the Option 18 field is not configured in a DHCPv6 message.

Format

dhcpv6 option18 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*

undo dhcpv6 option18 { [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format** | **format all** }

Parameters

Parameter	Description	Value
user-defined *text*	Indicates the user-defined format of the Option 18 field.	The value is a string of 1 to 251 characters. The details about the user-defined format string are provided in the Usage Guidelines.
vlan *vlan-id*	Specifies the outer VLAN ID. **NOTE** • If a VLAN is specified, only the format of the Option 18 field in DHCPv6 messages that belong to this VLAN is configured. If no VLAN is specified, the format of the Option 18 field in all DHCPv6 messages received by the interface is configured. • If the format of the Option 18 field is configured on an interface and the VLAN to which it belongs, the configuration on the interface takes effect. • This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN ID. **NOTE** This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
all	Deletes all formats of the Option 18 field.	-

Views

System view, VLAN view, Interface view, Port group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After the **dhcpv6 option18** { **insert** | **rebuild** } **enable** command is executed to enable the device to insert the Option 18 field to a DHCPv6 message, you can run the **dhcpv6 option18 format** command to configure the format of the Option 18 field in a DHCPv6 message.

You can use the following keywords to define the Option 18 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, Eth2/0/0. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.

 Copyright © Huawei Technologies Co., Ltd.

- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 18 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- The contents in quotation marks (" ") are encapsulated in an ASCII string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
  - A hexadecimal notation string can contain numerals, spaces, and % + keywords.
  - In a hexadecimal notation string, numbers are encapsulated in the Option 18 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
  - All the spaces in a hexadecimal character string are ignored.
  - By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
  - If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
  - A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
  - If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.

 Copyright © Huawei Technologies Co., Ltd.

- A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Example

Configure the format of the Option 18 field in a DHCPv6 message in VLAN 10.

```
<Huawei> system-view
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcpv6 option18 format user-defined "%length %svlan %5slot %3subslot %8port"
```

Configure the format of the Option 18 field in a DHCPv6 message on Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcpv6 option18 format user-defined "%length %svlan %5slot %3subslot
%8port"
```

Related Topics

19.14.21 dhcpv6 { option18 | option37 } enable

19.14.20 dhcpv6 option37 format

Function

The **dhcpv6 option37 format** command configures the format of the Option 37 field in a DHCPv6 message.

The **undo dhcpv6 option37 format** command restores the default format of the Option 37 field in a DHCPv6 message.

By default, the format of the Option 37 field is not configured in a DHCPv6 message.

Format

dhcpv6 option37 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*

undo dhcpv6 option37 { [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format** | **format all** }

Parameters

Parameter	Description	Value
user-defined *text*	Indicates the user-defined format of the Option 37 field.	The value is a string of 1 to 247 characters. The details about the user-defined format string are provided in the Usage Guidelines.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vlan *vlan-id*	Specifies the outer VLAN ID. **NOTE** • If a VLAN is specified, only the format of the Option 37 field in DHCPv6 messages that belong to this VLAN is configured. If no VLAN is specified, the format of the Option 37 field in all DHCPv6 messages received by the interface is configured. • If the format of the Option 37 field is configured on an interface and the VLAN to which it belongs, the configuration on the interface takes effect. • This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN ID. **NOTE** This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
all	Deletes all formats of the Option 37 field.	-

Views

System view, VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After the **dhcpv6 option37** { **insert** | **rebuild** } **enable** command is executed to enable the device to insert the Option 37 field to a DHCPv6 message, you can run the **dhcpv6 option37 format** command to configure the format of the Option 37 field in a DHCPv6 message.

You can use the following keywords to define the Option 37 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, Eth2/0/0. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.

 Copyright © Huawei Technologies Co., Ltd.

- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 37 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- The contents in quotation marks (" ") are encapsulated in an ASCII string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.

 Copyright © Huawei Technologies Co., Ltd.

- By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
- A hexadecimal notation string can contain numerals, spaces, and % + keywords.
- In a hexadecimal notation string, numbers are encapsulated in the Option 37 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
- All the spaces in a hexadecimal character string are ignored.
- By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
- If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
- A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
- If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
- A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Example

Configure the format of the Option 37 field in a DHCPv6 message in VLAN 10.

```
<Huawei> system-view
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcpv6 option37 format user-defined "%length %svlan %5slot %3subslot %8port"
```

Configure the format of the Option 37 field in a DHCPv6 message on Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcpv6 option37 format user-defined "%length %svlan %5slot %3subslot
%8port"
```

Related Topics

19.14.21 dhcpv6 { option18 | option37 } enable

 Copyright © Huawei Technologies Co., Ltd.

19.14.21 dhcpv6 { option18 | option37 } enable

Function

The **dhcpv6 { option18 | option37 } enable** command enables the device to insert the Option 18 or Option 37 field to a DHCPv6 message.

The **undo dhcpv6 { option18 | option37 } enable** command disables the device from inserting the Option 18 or Option 37 field to a DHCPv6 message.

By default, the device does not insert the Option 18 or Option 37 field to a DHCPv6 message.

Format

dhcpv6 { **option18** | **option37** } { **insert** | **rebuild** } **enable**

undo dhcpv6 { **option18** | **option37** } { **insert** | **rebuild** } **enable**

Parameters

Parameter	Description	Value
insert	Enables the device to insert the Option 18 or Option 37 field to a DHCPv6 message.	-
rebuild	Enables the device to forcibly insert the Option 18 or Option 37 field to a DHCPv6 message.	-

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The function of the Option 18 and Option 37 field is similar to the function of the Option 82 field (see the **dhcp option82 enable** command). The Option 18 field contains the port number of a client and the Option 37 field contains the MAC address of the client. A device inserts the Option 18 or Option 37 field to a DHCPv6 Request message to notify the DHCP server of the DHCPv6 client location. The DHCP server can properly assign an IP address and other configurations to the DHCPv6 client, ensuring DHCP client security.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If you run the **dhcpv6 { option18 | option37 } enable** command in the VLAN view, the command takes effect for all the DHCPv6 messages received from the specified VLAN. If you run the **dhcpv6 { option18 | option37 } enable** command in the interface view, the command takes effect for all the DHCPv6 messages received on the specified interface.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

If you run the **dhcpv6 { option18 | option37 } enable** command in the VLAN view, the command takes effect for all the DHCPv6 messages received from the specified VLAN. If you run the **dhcpv6 { option18 | option37 } enable** command in the interface view, the command takes effect for all the DHCPv6 messages received on the specified interface.

Example

Insert the Option 37 field to DHCPv6 Request messages sent by Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcpv6 option37 insert enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.22 dhcpv6 snooping relay-information enable

Function

The **dhcpv6 snooping relay-information enable** command enables Lightweight DHCPv6 Relay Agent (LDRA) for DHCPv6 snooping.

The **undo dhcpv6 snooping relay-information enable** command disables LDRA.

By default, LDRA is disabled for DHCPv6 snooping.

Format

dhcpv6 snooping relay-information enable [**trust**]

undo dhcpv6 snooping relay-information enable [**trust**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trust	Configures the device to trust the received Relay-Forward messages. If this parameter is not specified, the device does not trust the received Relay-Forward messages.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

In some scenarios, for example, interfaces in the same VLAN have different network access rights and QoS requirements, the DHCPv6 server must be able to detect user access locations, and assign corresponding access control and QoS policies. The DHCPv6 relay agent is usually configured on the gateway. The relay agent can record user access locations; however, if access devices are located between the relay agent and users, the relay agent cannot detect the access locations of users.

LDRA can meet the requirements of these scenarios. LDRA is configured on the user-side access device. The LDRA-enabled device can forward user access locations (such as the network-side interfaces on clients) to the DHCPv6 server. The DHCPv6 server delivers policies to users accordingly.

This command enables LDRA for DHCPv6 snooping and configures the handling methods for received Relay-Forward messages:

- Trust: The device forwards the received Relay-Forward messages to the DHCPv6 server. This method is usually used when multiple LDRA-enabled devices are directly connected. If the downstream LDRA-enabled device trusts the Relay-Forward messages from the upstream LDRA-enabled device, this method can be used.
- Untrust: The device discards the received Relay-Forward messages. This method is usually used when an LDRA-enabled device directly connects to users, and the users may send invalid Relay-Forward messages.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The LDRA function only records the client location information and forwards the information to the DHCPv6 server. The differentiated policies for IP address

 Copyright © Huawei Technologies Co., Ltd.

allocation, accounting, access control, and QoS are configured on the DHCPv6 server.

Example

Enable LDRA for DHCPv6 snooping in VLAN10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] dhcpv6 snooping relay-information enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.12 dhcp snooping enable no-user-binding

8.9.9 dhcpv6 interface-id format

19.14.23 display dhcp option82 configuration

Function

The **display dhcp option82 configuration** command displays the DHCP Option 82 configuration.

Format

display dhcp option82 configuration [**vlan** *vlan-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the DHCP Option 82 configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the DHCP Option 82 configuration on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can properly assign an IP address and other configurations to the DHCP client, ensuring DHCP client security.

After the Option 82 field is inserted to a DHCP message, run the **display dhcp option82 configuration** command to display the DHCP Option 82 configuration.

Example

Display all the DHCP Option82 configurations.

```
<Huawei> display dhcp option82 configuration
#
interface Ethernet2/0/0
 dhcp option82 subscriber-id format ascii 222
 dhcp option82 insert enable
 dhcp option82 encapsulation circuit-id
 dhcp option82 circuit-id format common
#
```

Table 19-149 Description of the **display dhcp option82 configuration** command output

Item	Description
interface *ifn*	Option 82 configuration on interface *ifn*.
dhcp option82 subscriber-id format ascii *text2*	The Sub6 suboption is inserted into the Option 82 field of DHCP messages. To specify the parameter, run the **19.14.32 dhcp option82 subscriber-id format** command.
dhcp option82 insert enable	The function of inserting Option 82 to DHCP messages is enabled and the insertion method is configured: • dhcp option82 rebuild enable: Rebuild mode • dhcp option82 insert enable: Insert mode To specify the parameter, run the **19.14.2 dhcp option82 enable** command.
dhcp option82 encapsulation circuit-id	The suboption inserted into the Option 82 field of DHCP messages is configured. To specify the parameter, run the **19.14.31 dhcp option82 encapsulation** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
dhcp option82 circuit-id format common	Format of the circuit-id suboption. To specify the parameter, run the **19.14.3 dhcp option82 format** command.

19.14.24 display dhcp snooping

Function

The **display dhcp snooping** command displays DHCP snooping running information.

Format

display dhcp snooping [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCP snooping running information on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
vlan *vlan-id*	Displays DHCP snooping running information in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcp snooping** command displays DHCP snooping running information. If no interface or VLAN is specified, global DHCP snooping running information is displayed. If an interface or a VLAN ID is specified, DHCP snooping running information about the interface or VLAN is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display global DHCP snooping running information.

```
<Huawei> display dhcp snooping
 DHCP snooping global running information   :
 DHCPv4 snooping                          : Enable
 DHCPv6 snooping                          : Enable
 Static user max number                    : 512
 Current static user number                : 0
 Dhcp user(dhcpv4/dhcpv6) max number       : 512
 Current dhcpv4 user number                : 0
 Current dhcpv6 user number                : 0
 Arp dhcp-snooping detect                  : Disable  (default)
 Alarm threshold                         : 100      (default)
 Bind-table autosave                       : Disable  (default)
 Offline remove mac-address                : Disable  (default)
 Client position transfer allowed          : Enable   (default)
 DHCPv6 confirm-client online detection    : Enable   (default)
 DHCPv6 client online detection times      : 3        (default)
 DHCPv6 client online detection interval   : 180      (default)

 DHCP snooping running information for VLAN 500   :
 DHCP snooping                            : Enable
 Dhcp user(dhcpv4/dhcpv6) max number       : 512
 Current dhcpv4 user number                : 0
 Current dhcpv6 user number                : 0
 Check dhcp-giaddr                         : Disable  (default)
 Check dhcp-chaddr                         : Disable  (default)
 Check dhcp-request                        : Disable  (default)

 DHCP snooping running information for interface Ethernet2/0/0   :
 DHCP snooping                            : Enable
 Trusted interface                       : No
 Dhcp user(dhcpv4/dhcpv6) max number       : 512
 Current dhcpv4 user number                : 0
 Current dhcpv6 user number                : 0
 Check dhcp-giaddr                         : Disable  (default)
 Check dhcp-chaddr                         : Disable  (default)
 Alarm dhcp-chaddr                         : Disable  (default)
 Discarded dhcp packets for check chaddr    : 0
 Check dhcp-request                        : Disable  (default)
 Alarm dhcp-request                        : Disable  (default)
 Alarm dhcp-reply                        : Disable  (default)
```

Table 19-150 Description of the **display dhcp snooping** command output

Item	Description
DHCPv4 snooping	Whether DHCPv4 snooping is enabled globally. To enable DHCP snooping, run the **19.14.11 dhcp snooping enable** command.
DHCPv6 snooping	Whether DHCPv6 snooping is enabled globally. To enable DHCP snooping, run the **19.14.11 dhcp snooping enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DHCP snooping	Whether DHCP snooping is enabled on the interface or in the VLAN. To enable DHCP snooping, run the **19.14.11 dhcp snooping enable** command.
Static user max number	Maximum number of static users.
Current static user number	Number of current static users.
Dhcp (dhcpv4/dhcpv6) max number	Shared specifications of the DHCPv4 snooping and DHCPv6 snooping binding tables.
Current dhcpv4 user number	Number of currently online DHCPv4 users.
Current dhcpv6 user number	Number of currently online DHCPv6 users.
Arp dhcp-snooping detect	Whether association between ARP and DHCP snooping is enabled. To enable association between ARP and DHCP snooping, run the **19.14.1 arp dhcp-snooping-detect enable** command.
Alarm threshold	Global alarm threshold for the number of discarded DHCP snooping messages. To set the global alarm threshold for the number of discarded DHCP snooping messages, run the **19.14.6 dhcp snooping alarm threshold** command.
Bind-table autosave	Whether a device is enabled to save the DHCP Snooping binding table. To enable the device to save the binding table, run the **19.14.16 dhcp snooping user-bind autosave** command.
Offline remove mac-address	Whether a device is enabled to delete MAC addresses of offline users.
Client position transfer allowed	Whether location transition is enabled for DHCP snooping users. To enable location transition for DHCP snooping users, run the **19.14.17 dhcp snooping user-transfer enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DHCPv6 confirm-client online detection	Whether the confirm-client probing function of DHCPv6 snooping is enabled.
DHCPv6 client online detection times	Number of times that the DAD NS messages are sent for DHCPv6 snooping to detect whether the user is online.
DHCPv6 client online detection interval	Interval at which the DAD NS messages are sent for DHCPv6 snooping to detect whether the user is online.
Trusted interface	Whether an interface is a trusted interface. To configure an interface as a trusted interface, run the **19.14.14 dhcp snooping trusted** command.
Check dhcp-giaddr	Whether a device is enabled to check the GIADDR field in a DHCP Request message. To enable the device to check the GIADDR field in a DHCP Request message, run the **19.14.7 dhcp snooping check dhcp-giaddr enable** command.
Check dhcp-chaddr	Whether a device is enabled to check whether the CHADDR field in a DHCP Request message matches the source MAC address in the Ethernet frame header. To enable the device to check whether the CHADDR field in a DHCP Request message matches the source MAC address in the Ethernet frame header, run the **19.14.8 dhcp snooping check mac-address enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alarm dhcp-chaddr	Whether a device is enabled to generate an alarm when the number of discarded DHCP Request messages with the CHADDR field different from the source MAC address in the Ethernet frame header exceeds the alarm threshold. To enable the device to generate an alarm when the number of discarded DHCP Request messages with the CHADDR field different from the source MAC address in the Ethernet frame header exceeds the alarm threshold, run the **19.14.5 dhcp snooping alarm enable** command.
Discarded dhcp packets for check chaddr	Number of messages discarded because the CHADDR field in the messages does not match the source MAC address in the Ethernet frame header.
Check dhcp-request	Whether an interface is enabled to check DHCP Request messages. To enable the interface to check DHCP Request messages, run the **19.14.9 dhcp snooping check user-bind enable** command.
Alarm dhcp-request	Whether a device is enabled to generate an alarm when the number of DHCP Request messages discarded within a specified period reaches the alarm threshold. To enable the device to generate an alarm when the number of DHCP Request messages discarded within a specified period reaches the alarm threshold, run the **19.14.5 dhcp snooping alarm enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alarm dhcp-reply	Whether a device is enabled to generate an alarm when an interface discards a DHCP Reply message from an untrusted interface. To enable the device to generate an alarm when an interface discards a DHCP Reply message from an untrusted interface, run the **19.14.5 dhcp snooping alarm enable** command.

19.14.25 display dhcp snooping configuration

Function

The **display dhcp snooping configuration** command displays the DHCP snooping configuration.

Format

display dhcp snooping configuration [**vlan** *vlan-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the DHCP snooping configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the DHCP snooping configuration on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping configuration is complete, run the **display dhcp snooping configuration** command to view the DHCP snooping configuration. If no VLAN or interface is specified, all the DHCP snooping configurations are displayed. If a VLAN or an interface is specified, only the DHCP snooping configuration in the VLAN or on the interface is displayed.

Example

Display all the DHCP snooping configurations.

```
<Huawei> display dhcp snooping configuration
#
dhcp snooping enable
#
vlan 3
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
#
interface Ethernet2/0/0
 dhcp snooping enable
#
```

Related Topics

19.14.11 dhcp snooping enable

19.14.9 dhcp snooping check user-bind enable

19.14.26 display dhcp snooping statistics

Function

The **display dhcp snooping statistics** command displays statistics on the received DHCP messages.

Format

display dhcp snooping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can use the **display dhcp snooping statistics** command to view statistics on the received DHCP messages of all types.

Example

Display statistics on the received DHCP messages.

```
<Huawei> display dhcp snooping statistics
 DHCP Snooping Statistics:

 Client Request:
  Dhcp Discover:                0
  Dhcp Request:                 0
  Dhcp Decline:                 0
  Dhcp Release:                 0
  Dhcp Inform:                  0
 Server Reply:
  Dhcp Offer:                   0
  Dhcp Ack:                     0
  Dhcp Nak:                     0
 Drop Packet:
  Dropped by mac-address check:   0
  Dropped by untrust reply:       0
  Dropped by request conflict:    0
  Dropped by untrust relay-forw:  0
 Delete DHCP snooping table:
  Receive release packet:         0
  Receive decline packet:         0
  Lease expired:                  0
  User command:                   0
  Client transferes:              0
  Interface down:                 0
  Arp detect:                     0
  Ucm notify:                     0
```

Table 19-151 Description of the display dhcp snooping statistics command output

Item	Description
Client Request	Number of packets sent by DHCP clients, including: • Number of DHCP Discover packets • Number of DHCP Request packets • Number of DHCP Decline packets • Number of DHCP Release packets • Number of DHCP Inform packets
Server Reply	Number of packets sent by the DHCP server, including: • Number of DHCP Offer packets • Number of DHCP ACK packets • Number of DHCP NAK packets
Drop Packet	Number of discarded packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dropped by mac-address check	Number of discarded DHCP messages whose MAC address is different from the CHADDR value.
Dropped by untrust reply	Number of untrusted reply packets that are discarded.
Dropped by request conflict	Number of packets that are discarded because the client and server MAC addresses conflict.
Dropped by untrust relay-forw	Number of untrusted Relay-Forward packets that are discarded.
Delete DHCP snooping table	Number of DHCP snooping binding entries deleted by the device.
Receive release packet	Number of DHCP snooping binding entries deleted by the device after the device receives DHCP release packets.
Receive decline packet	Number of DHCP snooping binding entries deleted by the device after the device receives DHCP decline packets.
Lease expired	Number of DHCP snooping entries deleted by the device because of lease expiry.
User command	Number of DHCP snooping binding entries deleted by using commands.
Client transferes	Number of DHCP snooping binding entries deleted because the client connects to another interface on the device.
Interface down	Number of DHCP snooping binding entries deleted because the port is shut down.
Arp detect	Number of DHCP snooping binding entries deleted due to ARP detection.
Ucm notify	Number of times the Ucm module requests DHCP snooping to delete user binding entries.

Related Topics

19.14.11 dhcp snooping enable

19.14.27 display dhcp snooping user-bind

 Copyright © Huawei Technologies Co., Ltd.

Function

The **display dhcp snooping user-bind** command displays the DHCP snooping binding table.

Format

display dhcp snooping user-bind { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the binding entry mapping a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
ip-address *ip-address*	Displays the binding entry mapping a specified IP address.	The value is in dotted decimal notation.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 4 digits.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After DHCP snooping is enabled, the device generates a DHCP snooping binding table. A binding entry contains the MAC address, IP address, number of the interface connected to the DHCP client, and VLAN ID on the interface. You can run the **display dhcp snooping user-bind** command to view the DHCP snooping binding table.

Example

Display information about the DHCP snooping binding table.

- Display all binding entries.

```
<Huawei> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
--------------------------------------------------------------------------------
10.1.28.141      78ac-d4b5-b858  10  /--  /--    Eth2/0/0       2008.10.17-07:31
--------------------------------------------------------------------------------
Print count:           1         Total count:          1
```

- Display detailed information about binding entries.

```
<Huawei> display dhcp snooping user-bind all verbose
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : 10.10.21.254
 MAC Address : 0200-0000-00e8
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : Eth2/0/0
 Lease       : 2008.01.20-19:54
 Gateway     : 10.10.21.1
 Server-ip   : 10.10.21.1
 IPSG Status : ineffective
--------------------------------------------------------------------------------
Print count:           1         Total count:          1
```

Table 19-152 Description of the **display dhcp snooping user-bind** command output

Item	Description
DHCP Dynamic Bind-table	DHCP snooping binding entries.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. • O: Outer VLAN • I: Inner VLAN • P: Vlan-mapping
IP Address	User IP address.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.
Lease	Time when the lease of the IP address used by the user expires.
Gateway	Gateway address.
Server-ip	IP addresses of the DHCP server.
IPSG Status	Whether the binding table is effective for IP packet checking after IP packet checking is enabled. The value can be: • effective • ineffective This field is invalid if IP packet checking is not enabled.

Related Topics

19.14.30 reset dhcp snooping user-bind

19.14.28 display dhcpv6 snooping user-bind

Function

The **display dhcpv6 snooping user-bind** command displays the DHCPv6 snooping binding table.

Format

display dhcpv6 snooping user-bind { { **interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the binding entry mapping a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
ipv6-address *ipv6-address*	Displays the binding entry mapping a specified IPv6 address.	The address is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table. If the parameter is not specified, brief information about the binding table is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping is enabled, the device generates a DHCP snooping binding table by listening to DHCP Request messages and Reply messages. A binding entry contains the MAC address, IP address, number of the interface connected to the

 Copyright © Huawei Technologies Co., Ltd.

DHCP client, and VLAN ID. You can run the **display dhcpv6 snooping user-bind** command to view the DHCPv6 snooping binding table.

Example

Display the DHCPv6 binding table.

- Display all the dynamic binding entries.

```
<Huawei> display dhcpv6 snooping user-bind all
DHCPV6 Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                  MAC Address     VSI/VLAN(O/I/P) Lease
------------------------------------------------------------------------------
FC00:1::1                   00d5-0191-02de  500 /--  /--    2008.10.01-00:26
------------------------------------------------------------------------------
print count:          1         total count:          1
```

- Display detailed information about the DHCPv6 binding table.

```
<Huawei> display dhcpv6 snooping user-bind all verbose
DHCPV6 Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
------------------------------------------------------------------------------
 IP Address  : FC00:1::1
 MAC Address : 00d5-0191-02de
 VSI         : --
 VLAN(O/I/P) : 101 /--  /--
 Interface   : Eth2/0/0
 Renew time  : 2016.12.12-15:00
 Expire time : 2016.12.12-15:00
 DadTimerId  : --
 DadPktNum   : --
 User State  : LIVE
------------------------------------------------------------------------------
Print count:          1         Total count:          1
```

Table 19-153 Description of the display dhcpv6 snooping user-bind command output

Item	Description
DHCPV6 Dynamic Bind-table	DHCPv6 Snooping dynamic binding table.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. • O: Outer VLAN • I: Inner VLAN • P: VLAN mapping
IP Address	User IPv6 address.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Renew time	Entry update time.
Expire time	Entry expiration time.
DadTimerId	Client probing timer ID.
DadPktNum	Remaining number of times a DAD NS packet can be transmitted.
User State	Status of a DHCPv6 snooping binding entry is as follows: • START • DETECTION • BOUND • LIVE

19.14.29 reset dhcp snooping statistics

Function

The **reset dhcp snooping statistics** command clears DHCP snooping statistic.

Format

reset dhcp snooping statistics { **global** | **interface** *interface-type interface-number* [**vlan** *vlan-id*] | **vlan** *vlan-id* [**interface** *interface-type interface-number*] }

Parameters

Parameter	Description	Value
global	Clears DHCP Snooping statistics on the globally.	-
interface *interface-type interface-number*	Clears DHCP Snooping statistics on the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
vlan *vlan-id*	Clears DHCP Snooping statistics in a specified VLAN. *vlan-id* specifies the ID of the VLAN.	*vlan-id* is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, if statistics are collected, you can run the **reset dhcp snooping statistics** command to clear the statistics.

Precautions

If both **interface** and **vlan** are specified, the specified interface must belong to the specified VLAN. The **reset dhcp snooping statistics** command clears DHCP Snooping statistics in the specified VLAN that the interface belongs to.

Example

Clear DHCP Snooping statistics on Eth2/0/0.

```
<Huawei> reset dhcp snooping statistics interface ethernet 2/0/0
```

Related Topics

19.14.24 display dhcp snooping

19.14.11 dhcp snooping enable

19.14.30 reset dhcp snooping user-bind

Function

The **reset dhcp snooping user-bind** command clears DHCP snooping binding entries.

Format

reset dhcp snooping user-bind [[**vlan** *vlan-id* | **interface** *interface-type interface-number*] * | **ip-address** [*ip-address*] | **ipv6-address** [*ipv6-address*]]

NOTE

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the keyword **ipv6-address**.

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Clears DHCP snooping binding entries mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Clears DHCP snooping binding entries mapping a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
ip-address	Clears DHCP snooping binding entries mapping IPv4 addresses.	-
ipv6-address	Clears DHCP snooping binding entries mapping IPv6 addresses.	-
ip-address	Clears DHCP snooping binding entries mapping a specified IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Clears DHCP snooping binding entries mapping a specified IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the mapping DHCP snooping binding entries are generated after DHCP users log in. The **reset dhcp snooping user-bind** command clears binding entries mapping a specified parameter. If no parameter is specified, all the binding entries are cleared.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If both **interface** *interface-type interface-number* and **vlan** *vlan-id* are configured, the interface specified by **interface** *interface-type interface-number* must have been added to the VLAN specified by **vlan** *vlan-id*. In this case, the command clears the DHCP snooping binding entries on a specified interface belonging to a certain VLAN.

Example

Clear DHCP snooping binding entries in VLAN 100.

```
<Huawei> reset dhcp snooping user-bind vlan 100
```

Related Topics

19.14.11 dhcp snooping enable
19.14.27 display dhcp snooping user-bind

19.14.31 dhcp option82 encapsulation

Function

The **dhcp option82 encapsulation** command configures suboptions inserted into the DHCP Option 82 field.

The **undo dhcp option82 encapsulation** command restores the default suboptions inserted into the DHCP Option 82 field.

By default, the circuit-id (CID), remote-id (RID), subscriber-id, and Sub9suboptions are inserted into the DHCP Option 82 field.

Format

dhcp option82 encapsulation { **circuit-id** | **remote-id** | **subscriber-id** } *

undo dhcp option82 encapsulation

Parameters

Parameter	Description	Value
circuit-id	Inserts the circuit-id suboption.	-
remote-id	Inserts the remote-id suboption.	-
subscriber-id	Inserts the subscriber-id (SID) suboption.	-

Views

System view, VLAN view, interface view, port group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

This function applies to a DHCP relay agent or a DHCP snooping-enabled device. The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security. The administrator can run this command to configure the device to insert one or more of the circuit-id suboption, remote-id suboption, subscriber-id suboption, and vendor-specific suboption in the Sub9 field into the DHCP Option 82 field. After the command is run, suboptions that are not configured to be inserted are not inserted into the DHCP Option 82 field by default.

Prerequisites

The DHCP function has been enabled in the system view using the **dhcp enable** command.

Example

Insert the circuit-id suboption into the DHCP Option 82 field.

```
<Huawei> system-view
[Huawei] dhcp option82 encapsulation circuit-id
```

19.14.32 dhcp option82 subscriber-id format

Function

The **dhcp option82 subscriber-id format** command inserts the Sub6 suboption into the DHCP Option 82 field of DHCP messages and configures the format of the Sub6 suboption.

The **undo dhcp option82 subscriber-id format** command cancels the configuration of the Sub6 suboption inserted into the DHCP Option 82 field of DHCP messages.

By default, the Sub6 suboption is not inserted into the DHCP Option 82 field of DHCP messages.

Format

dhcp option82 subscriber-id format { **ascii** *ascii-text* | **hex** *hex-text* }

undo dhcp option82 subscriber-id format

Parameters

Parameter	Description	Value
ascii *ascii-text*	Specifies the ASCII character string in the Sub6 field.	The value is an ASCII character string and contains fewer than 129 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hex *hex-text*	Specifies the HEX character string in the Sub6 field.	The value is in hexadecimal notation. The value can contain only digits 0 to 9, uppercase letters A to F, and lowercase letters a to f. If no space is included, the value length must be an even number smaller than 257.

Views

System view, Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an authentication system for wired Ethernet access based on DHCP, DHCP snooping, and Option82, a device can insert suboptions (suboption 1, suboption 2, suboption 6) into the Option 82 field in DHCP Request messages. These suboptions in DHCP Request messages help locate user devices. Unauthorized users cannot access the network by using static IP addresses or stealing accounts of authorized users. You can run the **dhcp option82 subscriber-id format** command to configure the Sub6 suboption.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

Configure the Sub6 suboption inserted into the DHCP Option 82 field of DHCP messages on GE0/0/1 and specify the ASCII character string in the Sub6 suboption.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] dhcp option82 subscriber-id format ascii hw
```

19.15 IP Source Guard Configuration Commands

NOTE

4GE-2S, 4ES2G-S,4ES2GP-S and 9ES2 cards do not support IPSG.

19.15.1 display dhcp static user-bind

 Copyright © Huawei Technologies Co., Ltd.

Function

The **display dhcp static user-bind** command displays information about a static binding table.

Format

display dhcp static user-bind { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays binding entries mapping a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
ip-address *ip-address*	Displays binding entries mapping a specified IP address.	The value is in dotted decimal notation.
mac-address *mac-address*	Displays binding entries mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays binding entries mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command is used to view information about a configured static binding table. The information includes the IP address, MAC address, VLAN information, and interface information.

Example

Display information about the static binding table.

```
<Huawei> display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address          MAC Address   VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.1.1.1            0001-0002-0003 10 /-- /--      Eth2/0/0
--------------------------------------------------------------------------------
Print count:     1     Total count:     1
```

Display detailed information about the static binding table.

```
<Huawei> display dhcp static user-bind all verbose
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : 10.21.21.254
 MAC Address : --
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : Eth2/0/0
--------------------------------------------------------------------------------
Print count:          1          Total count:          1
```

Table 19-154 Description of the display dhcp static user-bind command output

Item	Description
DHCP static Bind-table	Static DHCP binding entries. To configure a static DHCP binding table, run the **19.15.7 user-bind static** command.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. • O: Outer VLAN • I: Inner VLAN • P: Vlan-mapping
IP Address	User IP address.
MAC Address	User MAC address.
VSI	Name of the VSI that the online user belongs to.
VLAN(O/I/P)	Inner VLAN ID, outer VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.

 Copyright © Huawei Technologies Co., Ltd.

19.15.2 display dhcpv6 static user-bind

Function

The **display dhcpv6 static user-bind** command displays the IPv6 binding table.

Format

display dhcpv6 static user-bind { { **interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

NOTE

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the command.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays binding entries on the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
ipv6-address *ipv6-address*	Displays the binding entry mapping a specified IPv6 address.	The address is a 128-digit hexadecimal number, in the format of X:X::X:X.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

This command is used to view information about a configured DHCPv6 static binding table. The information includes the IPv6 address, MAC address, VLAN information, and interface information. If prefix delegation (PD) users exist on the network, the device generates an IPv6 prefix binding entry. The **display dhcpv6 static user-bind ipv6-prefix** command displays the static IPv6 prefix binding entries.

Example

Display the DHCPv6 static binding table.

```
<Huawei> display dhcpv6 static user-bind all
DHCPV6 static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address                MAC Address     VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
fc00:1::1                 0001-0002-0003  10  /--  /--    --
--------------------------------------------------------------------------------
print count:          1          total count:          1
```

Display detailed information about the DHCPv6 static binding table.

```
<Huawei> display dhcpv6 static user-bind all verbose
DHCPV6 static Bind-table:
--------------------------------------------------------------------------------
 IP Address  : fc00:1::1
 MAC Address : 0001-0002-0003
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : --
--------------------------------------------------------------------------------
print count:          1          total count:          1
```

Table 19-155 Description of the display dhcpv6 static user-bind command output

Item	Description
DHCPV6 static Bind-table	Static DHCPv6 binding entries. To configure a static DHCPv6 binding table, run the **19.15.7 user-bind static** command.
Flags:O - outer vlan ,I - inner vlan ,P - map vlan	VLAN ID. • O: Outer VLAN • I: Inner VLAN • P: Map VLAN
IP Address	User IPv6 address.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.

Related Topics

19.15.6 ip source check user-bind enable

19.15.3 display ip source check user-bind

Function

The **display ip source check user-bind** command displays the IPSG configurations.

Format

display ip source check user-bind { **vlan** *vlan-id* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the IP packet check configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the IP packet check configuration on a specified interface. The interface is specified by the interface type and number. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **display ip source check user-bind** command displays the IP packet check configuration on an interface or in a VLAN.

Example

Display the IP packet check configuration on Ethernet2/0/0.

```
<Huawei> display ip source check user-bind interface ethernet 2/0/0
 ip source check user-bind enable
 ip source check user-bind check-item ip-address
```

Table 19-156 Description of the display ip source check user-bind command output

Item	Description
ip source check user-bind enable	IP packet check is enabled. To enable IP packet check, run the **ip source check user-bind enable** command.
ip source check user-bind check-item ip-address	IP packet check items. To specify check items, run the **ip source check user-bind check-item** command.

Related Topics

19.15.4 ip source check user-bind check-item (interface view)

19.15.5 ip source check user-bind check-item (VLAN view)

19.15.6 ip source check user-bind enable

19.15.4 ip source check user-bind check-item (interface view)

Function

The **ip source check user-bind check-item** command configures IP packet check items on an interface.

The **undo ip source check user-bind check-item** command restores the default IP packet check items.

By default, the check items contain the IP address, MAC address, VLAN and interface information.

Format

ip source check user-bind check-item { **ip-address** | **mac-address** | **vlan** } *

undo ip source check user-bind check-item

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Checks whether the IP address of an IP packet matches a binding entry.	-
mac-address	Checks whether the MAC address of an IP packet matches a binding entry.	-
vlan	Checks whether VLAN information of an IP packet matches a binding entry.	-

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you check an IP packet against the binding table, run the **ip source check user-bind check-item (interface view)** command to specify items in the IP packet to be checked on a specified interface. When the device receives an IP packet, it checks the items against the binding table. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded. The optional check items of an IP packet contain the source IP address, source MAC address, and VLAN information. Interface information is a mandatory check item.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command in the interface view.

Precautions

When a large number of binding entries exist, it may take a long time to check IP packets, reducing forwarding efficiency.

This command is valid only for dynamic binding entries. The device checks the received packets against entries in the static binding table.

The **ip source check user-bind check-item (interface view)** command can only be used on Layer 2 interfaces, including Layer 2 Ethernet interfaces, Layer 2 GE interfaces, and Layer 2 Eth-Trunk interfaces.

Example

Enable IP packet check on Eth2/0/0 to check whether the IP address in the IP packet matches the binding entry.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip source check user-bind enable
```

 Copyright © Huawei Technologies Co., Ltd.

[Huawei-Ethernet2/0/0] **ip source check user-bind check-item ip-address**

Related Topics

19.15.6 ip source check user-bind enable

19.15.5 ip source check user-bind check-item (VLAN view)

Function

The **ip source check user-bind check-item** command configures IP packet check items in a VLAN.

The **undo ip source check user-bind check-item** command restores the default IP packet check items in a VLAN.

By default, the check items contain the IP address, MAC address, VLAN and interface information.

Format

ip source check user-bind check-item { **ip-address** | **mac-address** | **interface** } *

undo ip source check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Checks whether the IP address of an IP packet matches a binding entry.	-
mac-address	Checks whether the MAC address of an IP packet matches a binding entry.	-
interface	Checks whether interface information of an IP packet matches a binding entry.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you check an IP packet against the binding table, run the **ip source check user-bind check-item (VLAN view)** command to configure IP packet check items in a specified VLAN. When the device receives an IP packet, it checks the items against the binding table. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded. The optional check items of an IP

 Copyright © Huawei Technologies Co., Ltd.

packet contain the source IP address, source MAC address, and interface information. VLAN information is a mandatory check item.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command in the VLAN view.

Precautions

When a large number of binding entries exist, it may take a long time to check IP packets, reducing forwarding efficiency.

This command is valid only for dynamic binding entries. The device checks the received packets against entries in the static binding table.

Example

Enable IP packet check in VLAN 100 and check whether the IP address in the IP packet matches the binding entry.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] ip source check user-bind enable
[Huawei-vlan100] ip source check user-bind check-item ip-address
```

Related Topics

19.15.6 ip source check user-bind enable

19.15.6 ip source check user-bind enable

Function

The **ip source check user-bind enable** command enables IP packet check.

The **undo ip source check user-bind enable** command disables IP packet check.

By default, IP packet check is disabled.

Format

ip source check user-bind enable

undo ip source check user-bind enable

Parameters

None

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view, VLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Unauthorized users often send bogus packets with the source IP address and MAC address of authorized users to access or attack the network. Then authorized users cannot access stable and secure networks. To address this problem, you can configure IP packet check.

When IP packet check is enabled, the device checks the IP address, MAC address, VLAN information, and interface information against the binding table. You can run the **19.15.4 ip source check user-bind check-item (interface view)** or **19.15.5 ip source check user-bind check-item (VLAN view)** command to specify IP packet check items. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded.

Prerequisites

The IP packet check is based by binding table. So,

- The dynamic DHCP snooping binding table has been generated for DHCP users.
- The static binding table has been configured manually for users using static IP addresses.

Precautions

The **ip source check user-bind enable** command can only be used on Layer 2 interfaces, including Layer 2 Ethernet interfaces, Layer 2 GE interfaces, and Layer 2 Eth-Trunk interfaces.

Example

Enable IP packet check on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip source check user-bind enable
```

19.15.7 user-bind static

Function

The **user-bind static** command configures a static binding table.

The **undo user-bind static** command deletes a static binding table.

By default, no static binding table is configured.

Format

user-bind static { { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **mac-address** *mac-address* } * [**interface** *interface-type interface-number*] [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]

undo user-bind static [**interface** *interface-type interface-number* | { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **mac-address** *mac-address* | **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] *

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the keywords **ipv6-address** and **ce-vlan**.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface connected to a user in a static binding entry. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
ip-address	Indicates the static IPv4 address.	-
ipv6-address	Indicates the static IPv6 address.	-
start-ip [**to** *end-ip*]	Specifies the user IP address in a static binding entry. • *start-ip* specifies the first IP address. • **to** *end-ip* specifies the last IP address. The value of *end-ip* must be larger than the value of *start-ip*. *start-ip* and *end-ip* identify a VLAN range. If **to** *end-ip* is not specified, only the start IP address is added to the static binding entry. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	The IPv4 address is in dotted decimal notation in the format of X.X.X.X. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
mac-address *mac-address*	Specifies the user MAC address in a static binding entry.	The value is in hexadecimal notation. The value is in the format of H-H-H.
vlan *vlan-id*	Specifies the user VLAN ID in a static binding entry.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN tag of a QinQ packet in a static binding entry.	The value is an integer that ranges from 1 to 4094.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When DHCP snooping is enabled, a dynamic binding table is automatically generated for dynamic users. However, a static binding table cannot be generated for static users. If IP source guard is enabled but no static binding table is available, the device discards all static users' forwarding packets. To enable the device to forward static users' packets, run the **user-bind static** command to configure a static binding table.

Precautions

After a static binding table is configured and IP source guard is enabled, the device performs a match check on IP packets based on the configured binding entries. If the match check fails, the device discards the IP packets.

Example

Configure a static binding entry for a user in VLAN 2 with the IP address 10.1.1.1.

```
<Huawei> system-view
[Huawei] user-bind static ip-address 10.1.1.1 vlan 2
```

Related Topics

19.15.1 display dhcp static user-bind

19.16 URPF Configuration Commands

19.16.1 ipv6 urpf

Function

The **ipv6 urpf** command enables URPF check for IPv6 packets on an interface.

The **undo ipv6 urpf** command disables URPF check for IPv6 packets on an interface.

By default, URPF check for IPv6 packets is disabled on an interface.

Format

ipv6 urpf { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]

undo ipv6 urpf

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
loose	Indicates URPF loose check. When the source address of a packet exists in the FIB table, the packet is forwarded according to URPF regardless of whether the outbound interface of the matching entry is the same as the inbound interface of the packet.	-
strict	Indicates URPF strict check. A packet can be forwarded only when the source IP address of the packet exists in the FIB table and the inbound interface of the packet matches the outbound interface in the table.	-
allow-default-route	Allows special processing for the default route.	-
acl *acl-number*	Indicates URPF check for packets matching a specified ACL. URPF matches only source and destination IP addresses in ACL rules.	The value is an integer that ranges from 2000 to 3999. • The number of a basic ACL ranges from 2000 to 2999. • The number of an advanced ACL ranges from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

allow-default-route determines the processing mode for the default route:

 Copyright © Huawei Technologies Co., Ltd.

- If **allow-default-route** is not specified, a packet is discarded when the source IP address is not in the FIB table in either strict mode or loose mode.
- If **allow-default-route** is specified and the source IP address is not in the FIB enable, note the following points:
  - In strict mode, if the outbound interface of the default route is the same as the inbound interface of the packet, the packet passes the check and is forwarded. Otherwise, the packet is discarded.
  - In loose mode, the packet passes the check and is forwarded no matter whether the outbound interface of the default route is the same as the inbound interface of the packet.

Prerequisites

Run the **ipv6** command in the system view, and run the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 urpf** command cannot be used on Layer 2 interfaces.

Example

Enable URPF strict check for IPv6 packets on GE1/0/0 and allow special processing for the default route.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 urpf strict allow-default-route
```

19.16.2 urpf (interface view)

Function

The **urpf** command enables URPF check on the interface and configures the URPF check mode.

The **undo urpf** command disables URPF check on the interface.

By default, URPF check is not enabled on the interface.

Format

urpf { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]

undo urpf

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
loose	Indicates URPF check in loose mode. A packet can be forwarded as long as the source IP address of the packet exists in the routing table or ARP entry, regardless of whether the inbound interface of the packet matches the outbound interface in the table.	-
strict	Indicates URPF strict check in strict mode. A packet can be forwarded only when the source IP address of the packet exists in the routing table or ARP entry, and the inbound interface of the packet matches the outbound interface in the table.	-
allow-default-route	Allows special processing for the default route.	-
acl *acl-number*	Indicates URPF check for packets matching a specified ACL. URPF matches only source and destination IP addresses in ACL rules.	The value is an integer that ranges from 2000 to 3999. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Denial of Service (DoS) attack disables users from connecting to the server. DoS attacks aim to occupy many resources by sending a large number of connection requests to servers. The attacked servers cannot respond to authorized users.

URPF check enables the device to check the source IP address in the FIB table against the inbound interface of the packet. If the source IP address does not match the inbound interface of the packet, the packet is discarded. This prevents IP spoofing attacks, especially DoS attacks with bogus source IP address.

 Copyright © Huawei Technologies Co., Ltd.

You can configure **allow-default-route** in URPF check to determine processing mode for the default route.

- If **allow-default-route** is not specified, a packet is discarded when the source IP address is not in the FIB table in either strict mode or loose mode.
- If **allow-default-route** is specified and the source IP address is not in the FIB enable, note the following points:
  - In strict mode, if the outbound interface of the default route is the same as the inbound interface of the packet, the packet passes the check and is forwarded. Otherwise, the packet is discarded.
  - In loose mode, the packet passes the check and is forwarded no matter whether the outbound interface of the default route is the same as the inbound interface of the packet.

Example

Enable URPF strict check on GE1/0/0 and allow special processing for the default route.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] urpf strict allow-default-route
```

19.17 PKI Configuration Commands

19.17.1 auto-enroll

Function

The **auto-enroll** command enables automatic certificate enrollment and update.

The **undo auto-enroll** command disables automatic certificate enrollment and update.

By default, the automatic certificate enrollment and update are disabled.

Format

auto-enroll [*percent*] [**regenerate** [*key-bit*]] [**updated-effective**]

undo auto-enroll [**updated-effective**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
percent	Specifies the percentage of the certificate's validity period after which a new certificate is requested automatically.	The value is an integer that ranges from 10 to 100. The default value is 100. When the old certificate expires, the system requests a new certificate.
regenerate	Indicates the RSA key pair will be generated during certificate updates.	-
key-bit	Specifies the number of bits in the RSA key pair generated during certificate updates.	The value is an integer that ranges from 2048 to 4096. The default value is 2048.
updated-effective	Indicates that the certificate takes effect immediately after being updated. By default, an updated certificate takes effect only after the old one expires.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Automatic certificate enrollment: When the certificates are unavailable, will expire, or have expired, an entity automatically requests a new certificate or renews the certificate using the Simple Certification Enrollment Protocol (SCEP).

By default, the automatic certificate enrollment and update function is disabled. When a certificate has expired, you must request a certificate for an entity manually. You can still request a certificate for an entity manually when the automatic certificate enrollment and update function is enabled.

Precautions

- If you do not specify **regenerate**, the system uses the original RSA key pairs during automatic updates.

 Copyright © Huawei Technologies Co., Ltd.

- If you specify **regenerate**, the system generates new RSA key pairs during certificate updates for certificate requests and overwrites the original certificates and RSA key pairs with the new ones.
- After this command is run, the device checks whether the certificate has expired every 60 minutes. If the certificate has expired, the device updates the certificate.

Example

Enable automatic certificate enrollment and update for the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] auto-enroll 50 regenerate
```

19.17.2 ca-name

Function

The **ca-name** command configures the name of the CA in the PKI realm.

The **undo ca-name** command removes the name of the CA in the PKI realm.

By default, a PKI realm does not have a CA name.

Format

ca-name { *name-string* | **from-certificate filename** *file-name* }

undo ca-name

Parameters

Parameter	Description	Value
name-string	Specifies the name of the CA.	It is a string of 1 to 255 characters (including the quotation marks) and case sensitive. The value must start with and end with quotation marks (").
from-certificate filename *file-name*	Specifies the name of the CA certificate file through which the CA name is obtained.	It is a string of 1 to 64 characters and case insensitive.

Views

PKI realm view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After the CA name is specified in the PKI realm, associate the PKI realm with the specified CA. By using the CA name, you can determine the corresponding PKI realm and the check mode for the certificate revocation status.

You can directly specify the CA name by running the **ca-name** *name-string* command. Ensure that the CN, O, and OU in the CA name are in the same sequence as those in the subject name. Alternatively, you can obtain the CA name from the CA certificate by running the **ca-name from-certificate filename** *file-name* command. This avoids errors caused by manual operation.

Example

For the PKI realm **test**, specify the name of the CA.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] ca-name "CN=CA"
```

19.17.3 ca id

Function

The **ca id** command specifies a certificate authority (CA) trusted by a PKI realm.

The **undo ca id** command deletes the CA trusted by a PKI realm.

By default, no trusted CA is configured in a PKI realm.

Format

ca id *ca-name*

undo ca id

Parameters

Parameter	Description	Value
ca-name	Specifies the name of a CA trusted by a PKI realm.	The value is a string of 1 to 64 case-insensitive characters.

Views

PKI realm view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After the **ca id** command is executed to specify the CA trusted by the device, the CA then requests, obtains, revokes, or queries the device's certificate.

Example

Specify the CA **root_ca** trusted by the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] ca id root_ca
```

Related Topics

19.17.40 display pki realm
19.17.103 pki realm (system view)

19.17.4 cdp-url

Function

The **cdp-url** command configures the CRL distribution point (CDP) URL.

The **undo cdp-url** command deletes the configured CDP URL.

By default, no CDP URL is configured.

Format

cdp-url [**esc**] *url-addr*

cdp-url from-ca

undo cdp-url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url-addr	Specifies the CDP URL.	The value is a string starting with **http://** and consisting of 1 to 128 case-sensitive characters without spaces.
from-ca	Specifies that the CDP URL address is obtained from the CA certificate.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PKI entity needs to use HTTP to update CRL, it must set up a connection with the HTTP server based on CDP URL, and obtain the CRL from the HTTP server. By default, a PKI entity locates and downloads CRL based on the method (HTTP or LDAP) in the CDP information of the local certificate. If you do not want to download CRL based on the CDP URL in the local certificate, run this command to configure the PKI entity to obtain CDP URL from the CA certificate or manually configure the CDP URL.

When CRL is automatically updated by SCEP, you can also manually configure a CDP URL address.

Configuration Impact

Manually configuring a CDP URL address overwrites the CDP carried in the certificate. If the certificate does not contain CDP information and no CDP URL address is manually configured, the device requests the CRL from the CA server using SCEP.

Keyword **esc** only supports the URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

Set the CDP URL to http://10.1.1.1/certenroll/ca_root.crl.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl scep
[Huawei-pki-realm-d1] cdp-url http://10.1.1.1/certenroll/ca_root.crl
```

Set the CDP URL to http://www.***.com/certenroll/ca_root.crl.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl scep
[Huawei-pki-realm-d1] cdp-url http://www.***.com/certenroll/ca_root.crl
```

19.17.5 certificate-check

 Copyright © Huawei Technologies Co., Ltd.

Function

The **certificate-check** command sets the method of checking whether a certificate in the PKI realm is revoked.

The **undo certificate-check** command cancels the method of checking whether a certificate in the PKI realm is revoked.

By default, the system checks using CRLs whether a certificate in the PKI realm is revoked.

Format

certificate-check { { **crl** | **ocsp** } * [**none**] | **none** }

undo certificate-check

Parameters

Parameter	Description	Value
crl	Sets the check method to Certificate Revocation List (CRL).	-
ocsp	Sets the check method to Online Certificate Status Protocol (OCSP).	-
none	Indicates that the system does not check whether a certificate is revoked.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

After this command is executed, the PKI entity validates the peer certificate, for example, whether the peer certificate has expired and whether it is added to CRL.

The system supports the following methods to check whether a certificate in the PKI realm is revoked:

- CRL
  - If the CA server can function as a CDP, the certificate issued by CA contains the CDP information about obtaining the certificate CRL. The PKI entity then uses the specified method (HTTP or LDAP) to find the CRL from the specified location and download the CRL. If the CDP URL is configured in the PKI realm, the PKI entity obtains the CRL from the specified URL.

 Copyright © Huawei Technologies Co., Ltd.

  - If the CA does not support CDPs and no CDP URL is configured on the PKI entity, the PKI entity uses the SCEP protocol to obtain the CRL.

- OCSP

  The PKI entity can use OCSP to check certificate status online, and you do not need to frequently download CRLs.

  When two PKI entities use certificates to perform IPSec negotiation, they check the peer certificate status through OCSP in real time.

- None

  This mode is used when no CRL or OCSP server is available to the PKI entity or the PKI entity does not need to check the peer certificate status. In this mode, the PKI entity does not check whether a certificate has been revoked.

Select the following configurations:

- If the **certificate-check crl** command is configured for a certificate, the CRL mode is used.
- If the **certificate-check ocsp** command is configured for a certificate, the OCSP mode is used.
- If the **certificate-check crl none** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check ocsp none** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check crl ocsp** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the OCSP mode is used. If the OCSP mode is unavailable, the certificate is regarded as invalid.
- If the **certificate-check ocsp crl** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the CRL mode is used. If the CRL mode is unavailable, the certificate is regarded as invalid.
- If the **certificate-check crl ocsp none** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the OCSP mode is used. If the OCSP mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check ocsp crl none** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the CRL mode is used. If the CRL mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check none** command is configured for a certificate, the certificate is regarded as valid.

Precautions

After the **certificate-check crl** command is configured, if the device does not have the CRL file, the device fails the certificate verification, and the certificate becomes invalid.

It is not recommended that the none parameter be specified in the**certificate-check** command, because such a configuration poses security risks.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the certificate check method to **crl none** in PKI realm **test**. If the CRL mode is unavailable, the certificate is regarded as valid.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] certificate-check crl none
```

19.17.6 certificate auto-update enable

Function

The **certificate auto-update enable** command enables CMPv2-based automatic certificate update.

The **undo certificate auto-update enable** command disables CMPv2-based automatic certificate update.

By default, the CMPv2-based automatic certificate update is disabled.

Format

certificate auto-update enable

undo certificate auto-update enable

Parameters

None

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

If a certificate obtained through CMPv2 is about to expire, run this command to enable CMPv2-based automatic certificate update to ensure certificate validity. After the command is executed, the system performs checks (for example, referenced PKI entity, URL for the CMPv2 server, RSA key pair for CMPv2-based certificate application). The configuration is successful only when the conditions are met.

When the system detects that the remaining validity period of the local certificate has reached the value specified in **19.17.7 certificate update expire-time**, the system automatically initiates the certificate update request and decides whether to create an RSA key pair based on the **19.17.14 cmp-request rsa local-key-pair** configuration. After the new certificate is obtained, the system replaces the previous certificate and RSA key pair with the new ones. The replacement files

 Copyright © Huawei Technologies Co., Ltd.

include the files in device storage, certificate in memory, and configuration used in IKE negotiation.

Example

Enable CMPv2-based automatic certificate update.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] certificate auto-update enable
```

19.17.7 certificate update expire-time

Function

The **certificate update expire-time** command specifies when the certificate starts to update. The time is represented by a percentage of the total validity period.

The **undo certificate update expire-time** command restores the default certificate update time.

By default, the certificate is automatically updated when the validity period is only 50% left.

Format

certificate update expire-time *valid-percent*

undo certificate update expire-time

Parameters

Parameter	Description	Value
valid-percent	Specifies the remaining percentage of the validity period.	The value is an integer that ranges from 10 to 100. The default value is 50.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

If the automatic certificate update through CMPv2 is enabled, the system sends an update request to the CMPv2 server when the specified updated time is reached. This command sets the time (percentage of the total validity period) to update the certificate.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the automatic certificate update when the used time is 60% of the validity period of the certificate.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] certificate update expire-time 60
```

19.17.8 cmp-request authentication-cert

Function

The **cmp-request authentication-cert** command configures the certificate for identity authentication in the request through CMPv2.

The **undo cmp-request authentication-cert** command deletes the certificate for identity authentication in the request through CMPv2.

By default, no certificate for identity authentication in the request through CMPv2 is configured.

Format

cmp-request authentication-cert *cert-name*

undo cmp-request authentication-cert

Parameters

Parameter	Description	Value
cert-name	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run this command to configure the certificate for identity authentication if you need to apply for a certificate through CMPv2. For different requests through CMPv2, the required certificates are as follows:

- For Initialization Requests (IR), the required certificate is an external identity certificate.
- For certification requests (CR), the required certificate is the one that the CA has already issued to the device.

 Copyright © Huawei Technologies Co., Ltd.

- For the key update requests (KUR), the required certificate is the one that the CA has already issued to the device and is also the one to be updated.

Prerequisites

An identity authentication in the request through CMPv2 exists.

Example

Configure the certificate for identity authentication in the request through CMPv2.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request authentication-cert bb.cer
```

Related Topics

19.17.12 cmp-request origin-authentication-method

19.17.9 cmp-request ca-name

Function

The **cmp-request ca-name** command sets a CA name for the CMP session.

The **undo cmp-request ca-name** command deletes the CA name of the CMP session.

By default, no CA name is configured for a CMP session.

Format

cmp-request ca-name *ca-name*

undo cmp-request ca-name

Parameters

Parameter	Description	Value
ca-name	Indicates the name of the CA and is the field of subject in the CA certificate.	The value starts and ends with the quotation mark (") and is a string of 1 to 128 characters (including the quotation marks). A comma (,) is used to separate adjacent fields in the string.

Views

CMP session view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

A trusted authority enrolls and issues certificates to entities. Therefore, a trusted CA name must be configured.

The field order in the CA name must be the same as that in the actual CA certificate. Otherwise, the server regards the name as incorrect.

Example

Set the CA name for CMP session **test**.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request ca-name "C=cn,ST=beijing,L=shangdi,O=BB,OU=BB,CN=BB"
```

19.17.10 cmp-request entity

Function

The **cmp-request entity** command sets the entity name used to apply for certificate through CMPv2.

The **undo cmp-request entity** command deletes the entity name used to apply for certificate through CMPv2.

By default, the entity name used to apply for certificate through CMPv2 is not configured.

Format

cmp-request entity *entity-name*

undo cmp-request entity

Parameters

Parameter	Description	Value
entity-name	Specifies the entity name for certificate application.	The value must be an existing PKI entity name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

To apply for a certificate through CMPv2, create a CMP session and specify the entity name in the CMP session.

Prerequisites

1. A PKI entity has been created using the **pki entity** command.
2. A PKI entity common name has been created using the **common-name** command.

Precautions

The specified entity can be referenced only by one CMP session or PKI realm.

Example

Set the entity name the device uses when applying for a certificate through CMPv2 to **entity1**.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] common-name huawei
[Huawei-pki-entity-entity1] quit
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request entity entity1
```

Related Topics

19.17.79 pki entity

19.17.17 common-name

19.17.73 pki cmp session

19.17.11 cmp-request message-authentication-code

Function

The **cmp-request message-authentication-code** command configures the reference value and secret value of the message authentication code (MAC).

The **undo cmp-request message-authentication-code** command deletes the reference value and secret value of the MAC.

By default, the reference value and secret value of the MAC are not configured.

Format

cmp-request message-authentication-code *reference-value secret-value*

undo cmp-request message-authentication-code

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
reference-value	Specifies the reference value of the MAC.	The value is a string of 1 to 128 case-sensitive characters without spaces and question marks. If the character string is quoted by double quotation marks, it can contain spaces.
secret-value	Specifies the secret value of the MAC.	The length of the plaintext ranges from 1 to 128. The length of the encrypted ciphertext ranges from 48 to 188. The value is a case-sensitive character string without question marks.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

When a device is configured to use MAC for initial request (IR), you need to check the reference value and secret value of the MAC from the CMPv2 server in out-of-band mode, and then run this command to set the values on the device.

Example

Configure the reference value and secret value of the MAC.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request message-authentication-code 1234 123456
```

Related Topics

19.17.12 cmp-request origin-authentication-method

19.17.12 cmp-request origin-authentication-method

Function

The **cmp-request origin-authentication-method** command configures the authentication method used for initial request (IR) through CMPv2.

The **undo cmp-request origin-authentication-method** command restores the default authentication method used for IR through CMPv2.

By default, the authentication method used for IR through CMPv2 is MAC.

 Copyright © Huawei Technologies Co., Ltd.

Format

cmp-request origin-authentication-method { **message-authentication-code** | **signature** }

undo cmp-request origin-authentication-method

Parameters

Parameter	Description	Value
message-authentication-code	Indicates the MAC method for the IR.	-
signature	Indicates the signature method for the IR.	-

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

During the IR using CMPv2, a security protection measure needs to be taken:

- After you select the MAC method, run the **cmp-request message-authentication-code** command to configure the reference value and secret value. The device uses the reference value and secret value to protect messages during the IR.
- After you select the signature method, run the **cmp-request authentication-cert** command to configure the external certificate. The device uses the external certificate to protect signatures during the IR.

Example

Configure the authentication method used for IR through CMPv2.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request origin-authentication-method signature
```

19.17.13 cmp-request realm

Function

The **cmp-request realm** command specifies a PKI realm to which the CMPv2 server certificate belongs.

The **undo cmp-request realm** command deletes the specified PKI realm.

By default, no PKI realm is specified.

 Copyright © Huawei Technologies Co., Ltd.

Format

cmp-request realm *realm-name*

undo cmp-request realm

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of the imported certificate.	The value must be an existing PKI realm name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the CMPv2 mode is used, run the **cmp-request realm** command to specify a PKI realm to which the CMPv2 server certificate belongs.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command.

Example

Set a PKI realm name of the CMPv2 server certificate to **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request realm abc
```

19.17.14 cmp-request rsa local-key-pair

Function

The **cmp-request rsa local-key-pair** command configures the RSA key pair used for certificate application through CMPv2.

The **undo cmp-request rsa local-key-pair** command deletes the RSA key pair used for certificate application through CMPv2.

 Copyright © Huawei Technologies Co., Ltd.

By default, the RSA key pair used to apply for certificate through CMPv2 is not configured.

Format

cmp-request rsa local-key-pair *key-name* [**regenerate** [*key-bit*]]

undo cmp-request rsa local-key-pair

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair.	The value must be an existing RSA key pair name.
regenerate	Indicates that the RSA key pair is updated together with certificate update.	-
key-bit	Specifies the bits of the RSA key pair generated during the certificate update.	The value is an integer that ranges from 2048 to 4096. The default value is 2048.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the CMPv2 is used to apply for certificate, the certificate request message sent by the PKI entity to CA must contain public key information. Therefore, you need to configure an RSA key pair for certificate application through CMPv2.

Note the following during configurations:

- If **regenerate** is unspecified, the system uses the original RSA key pairs during automatic updates.
- If **regenerate** is specified, the system generates new RSA key pairs during certificate updates for the application for certificates and overwrites the original certificates and RSA key pairs with the new ones.

Prerequisites

The RSA key pair for certificate application has been created using the **19.17.106 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **19.17.95 pki import rsa-key-pair** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

One RSA key pair can be referenced only by one CMP session.

Example

Configure the RSA key pair to be referenced by CMP session **test** and update the RSA key pair during the certificate update.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....+++
.....
.....+++
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request rsa local-key-pair test regenerate 2048
```

Related Topics

19.17.106 pki rsa local-key-pair create
19.17.95 pki import rsa-key-pair

19.17.15 cmp-request server url

Function

The **cmp-request server url** command specifies the URL address of a CMPv2 server.

The **undo cmp-request server url** command deletes the URL address of a CMPv2 server.

By default, the URL of a CMPv2 server is not configured.

Format

cmp-request server url [**esc**] *url-addr*

undo cmp-request server url

Parameters

Parameter	Description	Value
esc	Specifies the entering of URLs in the ASCII code.	-
url-addr	Specifies the URL of the CMPv2 server.	The value is a string starting with **http://** and consisting of 1 to 128 case-insensitive characters without spaces.

Views

CMP session view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Configure an URL for the CMPv2 server before certificate application. Then the PKI entity sends a request message to the server's URL.

A user cannot enter command lines that include a question mark (?). Therefore, keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

Set the URL of the CMPv2 server for CMP session **test** to http://10.1.1.1:8080.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request server url http://10.1.1.1:8080
```

Set the URL of the CMPv2 server for CMP session **test** to http://www.***.com?page1\x3f.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request server url esc http://www.***.com\x3fpage1\\x3f
```

19.17.16 cmp-request verification-cert

Function

The **cmp-request verification-cert** command configures the certificate file for verifying the CA response signature.

The **undo cmp-request verification-cert** command deletes the certificate file for verifying the CA response signature.

By default, no certificate file for verifying the CA response signature is configured.

Format

cmp-request verification-cert *cert-file-name*

undo cmp-request verification-cert

Parameters

Parameter	Description	Value
cert-file-name	Specifies the certificate file name.	The value must be an existing certificate file name.

 Copyright © Huawei Technologies Co., Ltd.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is executed, the device uses the configured certificate to verify the CA response signature. This command configures the CA certificate.

If this command is not executed and the CA response mode is signature, the device constructs a certificate chain based on the certificates in the response messages sent by the device itself and CA to verify the CA response signature. If the MAC mode is set, the device uses the MAC to verify the CA response signature. That is, this command does not take effect.

Prerequisites

The certificate file for verifying the CA response signature exists.

Example

Configure the certificate file for verifying the CA response signature.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request verification-cert aa.der
```

19.17.17 common-name

Function

The **common-name** command configures a common name for an entity.

The **undo common-name** command cancels the configuration.

By default, a PKI entity does not have a common name.

Format

common-name *common-name*

undo common-name

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
common-name	Specifies the common name of an entity.	The value is a string of 1 to 64 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

After a PKI entity is created, a common name must be configured to uniquely identify the PKI entity.

After the common name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the common name of the PKI entity.

Example

Set the common name to **test** for an entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] common-name test
```

Related Topics

19.17.35 display pki entity

19.17.18 country (PKI entity view)

Function

The **country** command configures a country code for an entity.

The **undo country** command deletes the country code of a PKI entity.

By default, no country code is configured for a PKI entity.

Format

country *country-code*

 Copyright © Huawei Technologies Co., Ltd.

undo country

Parameters

Parameter	Description	Value
country-code	Specifies the country code of a PKI entity.	A country code must be two-character long. If the entered country code contains lower case letters, the system automatically changes the lower case letters into upper case letters when you create a certificate request file. You can query country codes in ISO3166. For example, CN is the legitimate country code of China, and US is the legitimate country code of the USA.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure the country code for the PKI entity, which is used as an alias of the entity.

After the country code is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this country code. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the country code of the PKI entity.

Example

Configure the country code to CN for a PKI entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] country CN
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.17.35 display pki entity

19.17.19 crl auto-update enable

Function

The **crl auto-update enable** command enables the automatic CRL update function.

The **undo crl auto-update enable** command disables the automatic CRL update function.

By default, automatic CRL update is enabled.

Format

crl auto-update enable

undo crl auto-update enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

To configure the automatic CRL update function, enable the function first.

Example

Enable the automatic certificate update function.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl auto-update enable
```

19.17.20 crl cache

Function

The **crl cache** command configures the device to use the cached CRL.

The **undo crl cache** command configures the device to retrieve the latest CRL each time.

 Copyright © Huawei Technologies Co., Ltd.

By default, the PKI realm is allowed to use cached CRLs.

Format

crl cache

undo crl cache

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The system overwrites the CRL in memory with the cached URL for certificate verification. If the PKI realm is not allowed to use cached CRL, the system must download the latest CRL every time to overwrite the CRL in memory.

Example

Allow the device to use the cached CRL in the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] crl cache
```

19.17.21 crl http

Function

The **crl http** command enables automatic CRL update using HTTP.

By default, the CRL is updated automatically using HTTP.

Format

crl http

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

This command is required when CRL is updated using HTTP.

When the device automatically updates the CRL using HTTP, ensure that there is sufficient space in the device storage for the CRL file.

Example

Configure the automatic CRL update using HTTP.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl http
```

19.17.22 crl ldap

Function

The **crl ldap** command configures the device to automatically update CRL using LDAP and specifies the attribute and identifier used to obtain CRL from the LDAP server.

The **undo crl ldap** command deletes the attribute and identifier used to obtain CRL from the LDAP server.

By default, the system automatically updates CRL using HTTP.

Format

crl ldap

crl ldap [**attribute** *attr-value*] **dn** *dn-value*

undo crl ldap dn

Parameters

Parameter	Description	Value
attribute *attr-value*	Specifies the attribute value that a device uses to obtain a CRL from an LDAP server.	The value is a string of 1 to 64 case-sensitive characters. By default, the value is **certificateRevocationList**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dn *dn-value*	Specifies the ID that a device uses to obtain a CRL from an LDAP server. The ID is generally composed of information, such as the user common name, organization name, country, or name of a certificate holder.	The value is a string of 1 to 128 case-sensitive characters, with spaces supported.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you use LDAP to automatically update a CRL, run the **crl ldap** command.

When a PKI entity automatically updates CRL using LDAP, it queries the attribute and identifier of LDAP server in the CRL query packet and obtains CRL from the LDAP server. In this situation, run the **crl ldap** [**attribute** *attr-value*] **dn** *dn-value* command to specify the attribute and identifier used to obtain CRL from the LADP server.

Precautions

The attribute and identifier used to obtain CRL from the LDAP server can be configured only after the **crl ldap** command is executed.

Before selecting the LDAP mode, ensure that the CF card or Hda1 has sufficient space for the CRL file. This effectively avoids upgrade failures.

Example

Configure automatic CRL update using LADP.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl ldap
[Huawei-pki-realm-d1] crl ldap attribute abcde dn test
```

19.17.23 crl scep

Function

The **crl scep** command configures a device to use SCEP to automatically update a CRL.

 Copyright © Huawei Technologies Co., Ltd.

By default, a device uses HTTP to automatically update a CRL.

Format

crl scep

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

This command is required when CRL is updated using SCEP.

Before the device automatically updates the CRL using SCEP, ensure that the device storage has sufficient space for the CRL file.

Example

Use SCEP to automatically update a CRL.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl scep
```

19.17.24 crl update-period

Function

The **crl update-period** command sets the interval for automatic CRL update.

The **undo crl update-period** command restores the default interval for automatic CRL update.

By default, the automatic CRL update interval is 8 hours.

Format

crl update-period *interval*

undo crl update-period

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a CRL is automatically updated.	The value is an integer that ranges from 1 to 720, in hours.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The CRL update interval is the interval at which a PKI entity using a certificate downloads a CRL from the CRL storage server. The CA/RA does not issue the CRL to an entity. Instead, the entity initiates CRL query to obtain a CRL.

Example

Set the interval at which a CRL is automatically updated to 21 hours.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl update-period 21
```

19.17.25 display ldap-server template

Function

The **display ldap-server template** command displays the configurations of an LDAP server template.

Format

display ldap-server template [*template-name*]

Parameters

Parameter	Description	Value
template-name	Specifies the name of an LDAP server template.	The value must be an existing LDAP server template name.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

If no template is specified, the configurations of all LDAP servers are displayed.

Example

Display the configurations of an LDAP server.

```
<Huawei> display ldap-server template
  ------------------------------------------------------------------------
  Server-template-name              : huawei
  Manager DN                        :
  Manager password                  :
  authentication-server             : -:0
  ------------------------------------------------------------------------
  Total of LDAP template :1
```

Table 19-157 Description of the **display ldap-server template** command output

Item	Description
Server-template-name	Name of an LDAP server template. To configure the name, run the **ldap-server template** command.
Manager DN	Administrator Base DN for accessing an LDAP server. To configure the administrator Base DN, run the **ldap-server authentication manager** command.
Manager password	Administrator password for accessing an LDAP server. To configure the administrator password, run the **ldap-server authentication manager** command.
authentication-server	IP address and port of the LDAP server. To configure the IP address and port, run the **ldap-server authentication** command.
Total of LDAP template	Total number of LDAP server templates.

19.17.26 display pki ca-capability

Function

The **display pki ca-capability** displays the CA capabilities of a PKI realm.

Format

display pki ca-capability realm *realm-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
realm *realm-name*	Indicates the name of a PKI realm.	The PKI realm name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display pki ca-capability** command displays the CA capabilities of a PKI realm.

If no command output is displayed, run the **pki get ca-capability realm** command in the diagnostic view to obtain the CA capabilities configured for the PKI realm.

Example

Display the CA capabilities of the PKI realm **asdf**.

```
<Huawei> display pki ca-capability realm asdf
 PKI CA Capabilities :
  GetNextCACert      :  ----
  POSTPKIOperation   :  ----
  Renewal            :  ----
  SHA-512            :  ----
  SHA-256            :  ----
  SHA-1              :  ----
  DES3               :  ----
```

Table 19-158 Description of the **display pki ca-capability** command output

Item	Description
PKI CA Capabilities	PKI CA capabilities.
GetNextCACert	Get next CA certificate.
POSTPKIOperation	Post PKI operation messages.
Renewal	Certificate renewal.
SHA-512	SHA-512 algorithm.
SHA-256	SHA-256 algorithm.
SHA-1	SHA-1 algorithm.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DES3	DES3 algorithm.

19.17.27 display pki cert-req

Function

The **display pki cert-req** command displays the content of a certificate request file.

Format

display pki cert-req filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of a certificate request file.	The certificate request file name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays content of a certificate request file, including the subject, public key algorithm, key modulus, attributes, and signature algorithm.

Example

Display the content of a certificate request file named **test.req**.

```
<Huawei> display pki cert-req filename test.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:01:cf:95:bb:fb:35:f0:3e:cd:1d:10:9e:11:
                    08:2e:77:48:ba:1b:e6:00:1b:43:30:56:f9:9a:6b:
                    ed:8b:fe:3e:03:57:38:02:48:88:e3:9b:39:d0:1c:
                    2b:8f:6a:9b:91:17:9b:ce:cb:fc:87:40:78:39:08:
                    1c:53:c3:71:cc:db:64:6f:ec:5a:cd:33:a5:68:5e:
```

 Copyright © Huawei Technologies Co., Ltd.

```
            e6:52:61:ad:a1:58:55:f0:a0:0f:db:ab:05:eb:a4:
            fe:e1:68:61:8c:af:2c:3a:34:95:d2:41:ee:09:e7:
            b0:fc:59:d9:f4:12:00:de:ab:14:b6:a3:fe:29:75:
            f7:dd:7b:aa:03:81:fc:ae:41:8c:e4:ad:e3:d9:65:
            d4:be:a0:c1:e0:43:8a:91:ad:20:7b:6f:12:25:6e:
            0d:67:7d:4c:fe:8d:1b:6d:f3:96:07:31:ed:73:d3:
            71:6b:51:18:64:bd:41:d6:18:2d:2d:86:b7:fa:26:
            eb:cc:cb:a3:0f:0b:61:22:fd:dd:5f:b4:4d:9b:7d:
            bc:fa:af:e6:95:d7:27:f1:60:31:56:83:58:2c:40:
            1a:5e:6a:94:63:aa:70:2f:9b:00:e0:a3:9e:fb:73:
            62:5e:1c:3c:5f:48:42:7c:26:8f:5f:cf:39:b9:5d:
            25:90:8e:6c:e0:04:ec:e2:1b:1f:a8:0d:d2:ef:20:
            41:79
        Exponent: 65537 (0x10001)
    Attributes:
      challengePassword       :******
    Requested Extensions:
      X509v3 Subject Alternative Name:
        IP Address:10.1.1.1, DNS:example.com, email:test@example.com
Signature Algorithm: sha256WithRSAEncryption
    71:e7:c0:5f:36:c9:16:eb:fc:0c:8e:d1:4f:3d:ee:25:6b:47:
    65:86:4b:89:ec:22:01:42:a5:0e:5c:aa:01:0a:57:a9:25:ba:
    1b:59:6d:77:5f:74:80:3b:af:f9:37:75:97:9a:ca:80:73:8b:
    36:14:2c:4b:9a:2f:53:5c:5b:4a:93:31:88:94:0f:4d:58:84:
    36:41:e8:a8:6c:cd:f0:bb:9f:51:50:b2:a4:40:f4:ec:37:c5:
    42:08:69:b5:c5:fd:af:3d:8a:aa:47:53:d3:ce:bc:76:ec:47:
    ca:36:90:0b:49:2b:2f:04:c4:1f:f1:12:b6:99:d0:f8:33:d8:
    08:d0:32:ac:ee:34:0f:07:ef:72:9f:6b:71:80:3e:8d:37:cc:
    ca:b5:c1:56:3d:65:c7:e6:99:1b:2b:53:01:69:f5:8a:18:05:
    d1:b1:48:3e:50:e0:4c:7f:db:dc:b7:cd:a2:37:f9:96:cd:0d:
    ee:61:c2:80:61:6b:99:c0:76:0d:ab:2c:46:ce:b7:aa:6a:12:
    72:b7:6f:64:cc:78:b7:16:bd:c5:32:45:79:42:cf:4c:28:91:
    ce:cd:7d:da:eb:2b:3a:cf:90:1f:61:5e:02:25:fe:3c:82:66:
    d4:e8:c7:f8:5e:84:2c:f6:b2:f0:ba:ee:7a:c1:9b:d4:68:02:
    a4:e3:27:89
```

Table 19-159 Description of the **display pki cert-req** command output

Item	Description
Certificate Request	Information about a certificate request file.
Data	Data of a certificate request file.
Version	Version of a certificate request file.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Subject	Subject of a certificate request file. The subject includes the following attributes: • C: country code of a PKI entity. It is configured using the **19.17.18 country (PKI entity view)** command. • ST: name of the state or province to which a PKI entity belongs. It is configured using the **19.17.120 state (PKI entity view)** command. • L: geographic area where a PKI entity is located. It is configured using the **19.17.61 locality** command. • O: organization to which a PKI entity belongs. It is configured using the **19.17.67 organization** command. • OU: department to which a PKI entity belongs. It is configured using the **19.17.66 organization-unit** command. • CN: common name of a PKI entity. It is configured using the **19.17.17 common-name** command.
Subject Public Key Info	Information about the subject public key of a certificate request file.
Public Key Algorithm	Public key algorithm.
Public-Key	RSA public key. It is configured using the **19.17.116 rsa local-key-pair** command.
Modulus	Key modulus.
Exponent	Key exponent.
Attributes	Attributes of a certificate request file.
challengePassword	The challenge password used in certificate application. It is configured using the **19.17.78 pki enroll-certificate** command.
Requested Extensions	Certificate request extension.
X509v3 Subject Alternative Name	Alternative name of the X.509v3 subject.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IP Address	IP address of a PKI entity. It is configured using the **19.17.53 ip-address** command.
DNS	DNS name of a PKI entity. It is configured using the **19.17.52 fqdn** command.
email	Email address of a PKI entity. It is configured using the **19.17.44 email** command.
Signature Algorithm	Signature algorithm. It is configured using the **19.17.47 enrollment-request signature message-digest-method** command.

19.17.28 display pki certificate

Function

The **display pki certificate** command displays the content about the CA or local certificate loaded to the device and OCSP server certificate.

Format

display pki certificate { **ca** | **local** | **ocsp** } **realm** *realm-name*

display pki certificate default { **ca** | **local** }

Parameters

Parameter	Description	Value
ca	Displays content about the CA certificate.	-
local	Displays content about the local certificate.	-
ocsp	Displays content about the Online Certificate Status Protocol (OCSP) server's certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The PKI realm name must already exist.
default	Specifies the content of the default built-in certificate.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command shows information about the CA certificate, local certificate, and OCSP server's certificate, including signature algorithm, issuer, validity period, subject, and subject public key.

Example

Display information about the CA certificate.

```
<Huawei> display pki certificate ca realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:f0:1a:f3:67:21:44:9a:4a:eb:ec:63:75:5d:d7:5f
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ca_root
        Validity
            Not Before: Jun  4 14:58:17 2015 GMT
            Not After : Jun  4 15:07:10 2020 GMT
        Subject: CN=ca_root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d9:5f:2a:93:cb:66:18:59:8c:26:80:db:cd:73:
                    d5:68:92:1b:04:9d:cf:33:a2:73:64:3e:5f:fe:1a:
                    53:78:0e:3d:e1:99:14:aa:86:9b:c3:b8:33:ab:bb:
                    76:e9:82:f6:8f:05:cf:f6:83:8e:76:ca:ff:7d:f1:
                    bc:22:74:5e:8f:4c:22:05:78:d5:d6:48:8d:82:a7:
                    5d:e1:4c:a4:a9:98:ec:26:a1:21:07:42:e4:32:43:
                    ff:b6:a4:bd:5e:4d:df:8d:02:49:5d:aa:cc:62:6c:
                    34:ab:14:b0:f1:58:4a:40:20:ce:be:a5:7b:77:ce:
                    a4:1d:52:14:11:fe:2a:d0:ac:ac:16:95:78:34:34:
                    21:36:f2:c7:66:2a:14:31:28:dc:7f:7e:10:12:e5:
                    6b:29:9a:e8:fb:73:b1:62:aa:7e:bd:05:e5:c6:78:
                    6d:3c:08:4c:9c:3f:3b:e0:e9:f2:fd:cb:9a:d1:b7:
                    de:1e:84:f4:4a:7d:e2:ac:08:15:09:cb:ee:82:4b:
                    6b:bd:c6:68:da:7e:c8:29:78:13:26:e0:3c:6c:72:
                    39:c5:f8:ad:99:e4:c3:dd:16:b5:2d:7f:17:e4:fd:
                    e4:51:7a:e6:86:f0:e7:82:2f:55:d1:6f:08:cb:de:
                    84:da:ce:ef:b3:b1:d6:b3:c0:56:50:d5:76:4d:c7:
                    fb:75
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.20.2:
                ...C.A
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C5
            X509v3 CRL Distribution Points:
```

 Copyright © Huawei Technologies Co., Ltd.

```
                Full Name:
                  URI:http://vasp-e6000-127.china.huawei.com/CertEnroll/ca_root.
crl
                  URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\ca_roo
t.crl

          1.3.6.1.4.1.311.21.1:
            ...
    Signature Algorithm: sha1WithRSAEncryption
        52:21:46:b8:67:c8:c3:4a:e7:f8:cd:e1:02:d4:24:a7:ce:50:
        be:33:af:8a:49:47:67:43:f9:7f:79:88:9c:99:f5:87:c9:ff:
        08:0f:f3:3b:de:f9:19:48:e5:43:0e:73:c7:0f:ef:96:ef:5a:
        5f:44:76:02:43:83:95:c4:4e:06:5e:11:27:69:65:97:90:4f:
        04:4a:1e:12:37:30:95:24:75:c6:a4:73:ee:9d:c2:de:ea:e9:
        05:c0:a4:fb:39:ec:5c:13:29:69:78:33:ed:d0:18:37:6e:99:
        bc:45:0e:a3:95:e9:2c:d8:50:fd:ca:c2:b3:5a:d8:45:82:6e:
        ec:cc:12:a2:35:f2:43:a5:ca:48:61:93:b9:6e:fe:7c:ac:41:
        bf:88:70:57:fc:bb:66:29:ae:73:9c:95:b9:bb:1d:16:f7:b4:
        6a:da:03:df:56:cf:c7:c7:8c:a9:19:23:61:5b:66:22:6f:7e:
        1d:26:92:69:53:c8:c6:0e:b3:00:ff:54:77:5e:8a:b5:07:54:
        fd:18:39:0a:03:ac:1d:9f:1f:a1:eb:b9:f8:0d:21:25:36:d5:
        06:de:33:fa:7b:c8:e9:60:f3:76:83:bf:63:c6:dc:c1:2c:e4:
        58:b9:cb:48:15:d2:a8:fa:42:72:15:43:ef:55:63:39:58:77:
        e8:ae:0f:34

Pki realm name: abc
Certificate file name: abc_ca.cer
Certificate peer name: -
```

Table 19-160 Description of the **display pki certificate** command output

Item	Description
The x509 object type is certificate.	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Subject	Subject of a certificate. The subject includes the following attributes: • C: country code of a PKI entity. • ST: name of the state or province to which a PKI entity belongs. • L: geographic area where a PKI entity is located. • O: organization to which a PKI entity belongs. • OU: department to which a PKI entity belongs. • CN: common name of a PKI entity.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm.
Public-Key	Public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Key Usage	X509v3 key usage.
X509v3 Basic Constraints	Basic constraints.
CA	Whether the CA can be trusted.
X509v3 Subject Key Identifier	Identifier of a subject key.
X509v3 CRL Distribution Points	CRL distribution points.
Full Name	Full name of CDP.
Pki realm name	PKI realm name.
Certificate file name	Certificate file name.
Certificate peer name	Certificate peer name.

19.17.29 display pki certificate built-in-ca

Function

The **display pki certificate built-in-ca** command displays the content of the SSL decryption certificate uploaded on the device.

 Copyright © Huawei Technologies Co., Ltd.

Format

display pki certificate built-in-ca

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command shows information about the SSL decryption certificate, including signature algorithm, issuer, validity period, subject, subject public key, PKI realm name, and certificate file name.

Example

Display information about the **built-in-ca** certificate.

```
<Huawei> display pki certificate built-in-ca
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f2:1c:74:f0:df:e0:2f:c6
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Validity
            Not Before: Oct 23 23:44:55 2015 GMT
            Not After : Oct 13 23:44:55 2055 GMT
        Subject: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b1:63:50:17:73:de:cc:9e:2b:41:fe:0e:58:28:
                    47:b7:ce:6b:77:5c:29:b1:3e:cf:d3:e0:53:63:1e:
                    21:cc:f6:11:34:7c:eb:8a:d7:08:b5:96:c4:0b:4a:
                    4d:33:6c:77:23:21:51:bb:10:d6:7d:d3:82:a0:6a:
                    f5:f6:8d:17:e0:f2:73:99:7b:c7:89:c8:fc:61:42:
                    0b:a5:d7:1a:11:47:ed:e1:5f:60:a6:c5:93:f0:07:
                    3f:73:fe:80:16:98:02:23:df:ab:04:85:13:25:32:
                    61:69:e8:f3:ab:a0:d8:e9:41:f8:c2:5f:14:9e:b7:
                    3b:49:1d:48:b4:b2:8d:bf:b9:00:ee:25:5d:7a:11:
                    a6:d3:23:61:99:ad:0f:54:be:00:a1:58:dd:d2:91:
                    ad:5c:6f:9d:d0:8c:e0:6f:a3:4e:df:ba:fd:b1:e3:
                    6f:1b:b3:1f:e6:42:91:1c:1a:4f:a3:a7:0e:3c:2c:
                    4c:f9:18:1f:9d:22:f8:09:da:ff:a7:7c:b8:77:20:
                    19:8a:90:d0:00:21:e4:1f:41:cc:f0:0c:ba:8f:23:
                    c3:9f:f9:ae:d8:49:95:be:75:49:7d:d7:d0:ce:3c:
                    28:27:e9:11:02:4d:c0:1a:d0:f7:38:7f:94:f8:9c:
                    9d:78:71:43:50:d3:05:01:07:18:f4:2f:c5:ec:96:
                    5d:d5
                Exponent: 65537 (0x10001)
```

 Copyright © Huawei Technologies Co., Ltd.

```
      X509v3 extensions:
          X509v3 Subject Alternative Name:
              IP Address:10.1.1.1, DNS:example.com, email:test@example.com
          X509v3 Basic Constraints: critical
              CA:TRUE
          X509v3 Key Usage: critical
              Certificate Sign, CRL Sign
          X509v3 Subject Key Identifier:
              3F:D2:BC:62:6B:F5:10:29:C4:59:9D:B9:71:A7:EB:B1:C4:16:91:9F
          Netscape Cert Type:
              SSL CA
          Netscape Comment:
              example comment extension
    Signature Algorithm: sha1WithRSAEncryption
        89:d5:47:31:23:c3:f9:df:fd:96:c5:38:fb:1e:b5:52:00:bd:
        21:fd:f0:18:af:8e:e8:01:b7:e6:b3:a1:0e:51:4b:61:4d:d5:
        52:1e:60:60:6a:67:9f:82:90:e3:1d:97:36:8f:c4:30:20:f4:
        14:58:4c:78:61:3c:4a:d4:0f:98:a9:05:e0:b5:cb:6a:78:eb:
        c6:40:9d:00:7b:31:8d:0e:21:72:db:31:34:83:5d:e5:42:98:
        85:09:6d:1e:c5:23:ce:e3:72:46:67:79:4b:1b:18:ba:cb:5e:
        ba:08:ee:0e:24:e5:58:07:0c:2e:b8:cf:e6:6b:09:67:76:80:
        e5:0e:66:a2:cb:3a:a1:bc:56:27:1c:1b:fd:5a:b5:ad:9f:a4:
        32:2b:32:3e:9a:9d:f5:04:ee:e5:e1:1c:76:8a:c2:45:f1:3e:
        8c:da:ab:f6:cf:82:d0:b3:4c:91:7a:c8:ad:b5:2c:28:54:e0:
        79:40:b6:b5:f1:6f:92:23:4d:94:8b:20:0d:92:86:43:98:17:
        d5:9b:b0:7f:99:f2:f1:df:0f:d3:f2:5c:9d:35:bc:64:25:13:
        39:62:ba:98:cb:cc:6a:08:fc:2c:86:2e:2e:91:80:8b:3e:27:
        14:f7:45:fe:9f:f8:1a:87:05:c9:21:c3:61:d1:69:82:e3:05:
        5c:44:c5:82

Pki realm name: -
Certificate file name: buzzcer
Certificate peer name: -
```

Table 19-161 Description of the **display pki certificate built-in-ca** command output

Item	Description
The x509 object type is certificate	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Subject	Certificate subject. The subject includes the following attributes: • C: country code of a PKI entity. It is configured using the **19.17.18 country (PKI entity view)** command. • ST: name of the state or province to which a PKI entity belongs. It is configured using the **19.17.120 state (PKI entity view)** command. • L: geographic area where a PKI entity is located. It is configured using the **19.17.61 locality** command. • O: organization to which a PKI entity belongs. It is configured using the **19.17.67 organization** command. • OU: department to which a PKI entity belongs. It is configured using the **19.17.66 organization-unit** command. • CN: common name of a PKI entity. It is configured using the **19.17.53 ip-address** command.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm. It is configured using the **19.17.106 pki rsa local-key-pair create** command.
Public-Key	RSA public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Subject Alternative Name	Alternative name of the X.509v3 subject.
IP Address	IP address of the PKI entity. It is configured using the **19.17.53 ip-address** command.
DNS	DNS name of a PKI entity. It is configured using the **19.17.52 fqdn** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
email	Email address of a PKI entity. It is configured using the **19.17.44 email** command.
X509v3 Basic Constraints	Basic constraints.
CA	Whether the CA can be trust.
X509v3 Key Usage	X.509v3 key use.
X509v3 Subject Key Identifier	Identifier of a X.509v3 subject key.
Netscape Cert Type	Netscape Certificate Type.
Netscape Comment	Netscape Comment.
Signature Algorithm	Signature algorithm.
Pki realm name	PKI realm name. It is configured using the **19.17.103 pki realm (system view)** command.
Certificate file name	Name of a certificate file. It is configured using the **19.17.86 pki generate built-in-ca certificate** command.
Certificate peer name	Name of a certificate peer. It is configured using the **19.17.92 pki import-certificate peer** command.

19.17.30 display pki certificate enroll-status

Function

The **display pki certificate enroll-status** command displays the certificate enrollment status.

Format

display pki certificate enroll-status [**realm** *realm-name*]

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The PKI realm name must already exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pki certificate enroll-status** command displays the certificate enrollment status.

Example

Display the certificate enrollment status.

```
<Huawei> display pki certificate enroll-status realm abc
 Certificate Request Transaction 1
    Status: Pending
    Key Usage: ENC&SIG
    Entity name: test
    Remain polling count: 1
    Next polling after : 35 seconds
<Huawei> display pki certificate enroll-status realm abc
 info: No certificate request transaction in realm abc.
```

Table 19-162 Description of the **display pki certificate enroll-status** command output

Item	Description
Certificate Request Transaction	Certificate enrollment request process.
Status	Certificate enrollment status. Pending: A certificate is being enrolled.
Key Usage	Functions of a certificate public key: • ENC: The public key is used for encryption. • SIG: The public key is used for signature.
Entity name	Entity name.
Remain polling count	Number of times a certificate enrollment request can be initiated again.
Next polling after	Next time a certificate enrollment request is initiated.
No certificate request transaction	There is no certificate enrollment request process.

 Copyright © Huawei Technologies Co., Ltd.

19.17.31 display pki certificate filename

Function

The **display pki certificate** command displays the content about the CA or local certificate loaded to the device and OCSP server certificate.

Format

display pki certificate filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about the certificate including signature algorithm, issuer, validity period, subject, and subject public key.

Example

Display information about the certificate ca.cer.

```
<Huawei> display pki certificate filename ca.cer
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      f3:a3:3a:46:f6:09:8d:18
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=CN, ST=JS, L=NJ, O=HW, OU=VPN, CN=CA-210235G7G410FB000060
    Validity
      Not Before: May 16 11:48:04 2017 GMT
      Not After : May 14 11:48:04 2027 GMT
    Subject: C=CN, ST=JS, L=NJ, O=HW, OU=VPN, CN=CA-210235G7G410FB000060
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:ba:cc:ef:2f:55:9c:d0:09:c5:1b:d2:52:63:92:
          c8:f0:88:ed:1b:88:f1:e4:3c:90:07:85:01:8c:d5:
          80:d9:91:ef:64:e9:79:0c:7d:0e:b9:6c:00:a2:72:
          e2:1b:aa:9b:2d:11:6b:6f:2d:de:5d:58:22:cf:9e:
          2f:7d:f1:ad:71:e9:25:0e:bc:26:f1:77:57:02:3d:
          7f:09:8f:49:63:ae:11:75:57:65:a0:bd:9c:94:c6:
```

 Copyright © Huawei Technologies Co., Ltd.

```
            df:21:f7:c8:5a:4d:5e:f8:5e:84:b0:b0:fd:a6:c7:
            e0:78:d1:1c:8a:55:d9:e9:66:1c:e5:4e:ce:88:dd:
            fa:0f:60:d0:7e:86:a1:ec:b1:34:aa:f7:dd:72:c6:
            0a:90:c7:4a:6b:a0:86:01:30:b6:6f:23:ff:ce:ae:
            39:fb:de:18:ce:2f:b9:d7:17:09:8c:29:19:34:7a:
            69:75:dc:ee:bf:2e:d4:93:fb:f6:a6:5b:f8:2a:6d:
            fe:bd:f4:8b:30:49:5c:a8:94:76:12:9d:64:78:4a:
            48:d3:2d:63:da:0a:79:b2:ee:8e:2d:5a:a0:71:99:
            cf:b9:68:77:d3:d9:cf:12:64:80:bb:42:8c:28:1f:
            d9:bf:7c:4b:8f:39:1e:dc:92:a4:ff:8e:b3:02:58:
            c5:79:96:f2:a1:f9:17:cb:ea:49:57:b0:b0:3c:af:
            db:19
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Subject Key Identifier:
            83:08:A4:F4:BC:EC:1B:B6:7D:B0:27:F6:10:47:77:AA:2A:66:59:D5
        Netscape Cert Type:
            SSL CA
Signature Algorithm: sha256WithRSAEncryption
    1e:6b:2a:76:7e:8e:b0:0e:72:4e:02:53:b0:77:0d:13:28:4e:
    c3:e5:f8:0b:76:fd:56:2c:e6:5b:d1:f8:48:19:17:95:1a:79:
    5e:d9:50:b9:68:bd:36:c4:ce:7b:ce:0c:98:55:b1:44:9f:20:
    66:66:33:3c:b5:40:ad:50:c8:64:1c:07:0e:08:42:72:88:35:
    d4:af:f0:8d:5d:64:90:5d:ec:f0:5c:07:76:10:ed:9b:22:18:
    ef:44:4e:c2:29:32:40:68:fe:04:dc:0e:f6:2b:25:c2:73:f5:
    9b:64:df:25:56:c6:bb:6e:a4:2f:07:b3:9d:c0:18:60:72:cb:
    51:62:94:ee:f7:21:0a:a0:92:58:a1:bf:c8:30:0e:0c:0a:91:
    cb:f4:8f:07:52:ba:df:25:88:8a:b3:3f:f0:68:fa:4c:b7:31:
    c8:97:e0:49:08:8a:74:fc:c2:90:d7:3c:0b:00:38:90:3b:19:
    ab:66:96:24:1f:86:b9:62:49:6d:9c:2d:02:99:38:bb:96:b6:
    dd:0f:3c:6e:24:7b:3d:1e:77:58:e7:46:2b:42:cc:14:6a:a4:
    16:45:ed:3c:b1:d6:30:94:c0:30:d0:46:fa:bc:da:9a:2b:f1:
    fa:f3:df:1b:84
```

Table 19-163 Description of the **display pki certificate filename** command output

Item	Description
The x509 object type is certificate.	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Subject	Subject of a certificate. The subject includes the following attributes: • C: country code of a PKI entity. • ST: name of the state or province to which a PKI entity belongs. • L: geographic area where a PKI entity is located. • O: organization to which a PKI entity belongs. • OU: department to which a PKI entity belongs. • CN: common name of a PKI entity.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm.
Public-Key	Public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Basic Constraints	X.509v3 basic constraints.
CA	Whether the CA can be trusted.
X509v3 Subject Key Identifier	Identifier of a X.509v3 subject key.
X509v3 Key Usage	X509v3 key usage.
Netscape Cert Type	Netscape certificate type.

19.17.32 display pki cmp statistics

Function

The **display pki cmp statistics** command displays the statistics on CMP sessions.

Format

display pki cmp statistics [**session** *session-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
session *session-name*	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays statistics on CMP sessions, including the number of sent IR packets, sent CR packets, sent KUR packets, and received IP packets.

If a CMP session is specified, the statistics of the session is displayed. If no CMP session is specified, the statistics of all sessions is displayed.

Example

Display statistics on CMP session test.

```
<Huawei> display pki cmp statistics session test
 CMP Context Name: test
 Ir Send Counts        : 0
 Cr Send Counts        : 0
 Kur Send Counts       : 0
 PollReq Send Counts   : 0
 Ip Receive Counts     : 0
 Cp Receive Counts     : 0
 Kup Receive Counts    : 0
 PollRep Receive Counts: 0
```

Table 19-164 Description of the **display pki cmp statistics** command output

Item	Description
CMP Context Name	Name of the CMP session.
Ir Send Counts	Total number of IR packets sent during the session.
Cr Send Counts	Total number of CR packets sent during the session.
Kur Send Counts	Total number of KUR packets sent during the session.
PollReq Send Counts	Total number of requests sent in polling mode during the session.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ip Receive Counts	Number of IP packets received during the session.
Cp Receive Counts	Number of CP packets received during the session.
Kup Receive Counts	Number of KUP packets received during the session.
PollRep Receive Counts	Number of responses received in polling mode during the session.

19.17.33 display pki credential-storage-path

Function

The **display pki credential-storage-path** command displays the default path where a PKI certificate is stored.

By default, the certificate file is stored in sd1:/.

Format

display pki credential-storage-path

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pki credential-storage-path** command displays the default path where a PKI certificate is stored.

Example

Display the default path where a PKI certificate is stored.

```
<Huawei> display pki credential-storage-path
 The pki credential-storage-path is sd1:/ .
```

 Copyright © Huawei Technologies Co., Ltd.

19.17.34 display pki crl

Function

The **display pki crl** command displays the content of the CRL in the device.

Format

display pki crl { **realm** *realm-name* | **filename** *filename* }

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of the PKI realm associated with the CRL.	The PKI realm name must already exist.
filename *filename*	Specifies the file name of the certificate to be imported.	The certificate file name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about local CRL, including signature algorithm, issuer, update time, revoked certificate, CRL sequence number, and revocation time.

Example

Display information about the CRL associated with the PKI realm **abc**.

```
<Huawei> display pki crl realm abc
 The x509 object type is CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: /CN=ca_root
        Last Update: Dec 15 08:24:28 2015 GMT
        Next Update: Dec 22 20:44:28 2015 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C
5
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 CRL Number:
                365
            1.3.6.1.4.1.311.21.4:
151222083428Z   .
```

 Copyright © Huawei Technologies Co., Ltd.

```
Revoked Certificates:
    Serial Number: 28C63371000000003E04
        Revocation Date: Dec 15 08:34:27 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 28C2AB44000000003E01
        Revocation Date: Dec 15 08:30:35 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 2364247C000000003D48
        Revocation Date: Dec 14 07:29:05 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 23627E0F000000003D47
        Revocation Date: Dec 14 07:27:29 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 2360F397000000003D46
        Revocation Date: Dec 14 07:25:48 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Signature Algorithm: sha1WithRSAEncryption
         7a:71:54:d1:66:13:6f:9f:62:03:ac:9a:5f:42:10:15:87:46:
         e2:a1:49:0f:44:19:ce:ed:6f:c3:0e:9f:31:fe:62:d5:08:0b:
         a4:a7:7e:80:4d:9a:5b:a9:55:5c:1a:73:30:62:48:e1:28:0e:
         5b:bd:ae:04:7e:83:36:43:62:fc:f7:12:0d:f9:f6:ac:2b:be:
         9c:50:6c:67:19:43:12:31:67:c2:06:31:97:e1:34:75:1c:87:
         53:5f:e6:15:a1:33:ad:00:e7:14:68:59:05:67:28:78:a0:91:
         49:7b:ab:87:9f:9e:53:18:4b:54:53:1c:b7:1c:2d:3e:b3:57:
         63:95:1d:01:29:9e:6c:41:07:40:2d:28:d8:82:7b:d6:22:e6:
         0d:0c:4c:af:84:96:8e:f1:29:28:d4:9e:1c:37:3b:1b:2e:34:
         a7:15:e3:29:d1:c0:69:0a:7f:24:b1:ce:00:f1:b3:da:ef:8a:
         1b:14:36:f9:14:6c:b0:66:86:a8:92:95:fc:e3:78:aa:d6:d0:
         cb:4d:26:b4:bc:41:c4:47:19:d0:2a:0c:ac:c6:aa:95:c2:03:
         33:8a:39:45:3e:c3:ad:46:7d:8a:03:4d:08:e2:d0:9a:ae:39:
         fa:8d:61:d0:1c:6c:03:d4:48:2e:4d:37:60:a1:06:a4:ea:c8:
         0d:20:59:c2

Pki realm name: abc
CRL file name: abc.crl
```

Table 19-165 Description of the **display pki crl** command output

Item	Description
The x509 object type is CRL	x509 object type is CRL.
Certificate Revocation List (CRL)	Information about the CRL.
Signature Algorithm	Algorithm of signature.
Issuer	Information of issuer.
Last Update	Last time the CRL has been updated.
Next Update	Next time the CRL will be updated.
CRL extensions	CRL extended attribute.
X509v3 Authority Key Identifier	X509v3 authority key identifier.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
X509v3 CRL Number	X509v3 CRL number.
Revoked Certificates	Certificate that is revoked.
Serial Number	Serial number of the CRL.
Revocation Date	Date when the certificate was revoked.
CRL entry extensions	CRL entry extensions.
X509v3 CRL Reason Code	Reason why CRL is revoked.
Signature Algorithm	Signature algorithm. It is configured using the **19.17.47 enrollment-request signature message-digest-method** command.
Pki realm name	PKI realm name. It is configured using the **19.17.103 pki realm (system view)** command.
CRL file name	CRL file name. It is configured using the **19.17.93 pki import-crl** command.

19.17.35 display pki entity

Function

The **display pki entity** command displays information about PKI entities.

Format

display pki entity [*entity-name*]

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity. If the *entity-name* parameter is not specified, information about all entities is displayed.	The value must be an existing PKI entity name.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command displays information about PKI entities, including names, common names, countries, province, and location where the entities reside, and organizations to which entities belong.

Example

Display information about all PKI entities.

```
<Huawei> display pki entity
PKI Entity Information:

  Entity Name      : a
  Common name      : chi
  Country          : -
  State            : A
  Locality         : -
  Organization     : A
  Organization unit: -
  FQDN             : www. e
  IP address       : -
  Email            : -
  Serial-number    : -
 Total Number: 1
```

Table 19-166 Description of the **display pki entity** command output

Item	Description
PKI Entity Information	Information of the PKI entity.
Entity Name	Entity name. It is configured using the **19.17.79 pki entity** command.
Common name	Common name of the entity. It is configured using the **19.17.17 common-name** command.
Country	Country where a PKI entity resides. It is configured using the **19.17.18 country (PKI entity view)** command.
State	Province where a PKI entity resides. It is configured using the **19.17.120 state (PKI entity view)** command.
Locality	Location of a PKI entity. It is configured using the **19.17.61 locality** command.
Organization	Organization to which a PKI entity belongs. It is configured using the **19.17.67 organization** command.
Organization unit	Organization unit to which a PKI entity belongs. It is configured using the **19.17.66 organization-unit** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
FQDN	FQDN name of a PKI entity. It is configured using the **19.17.52 fqdn** command.
IP address	IP address of a PKI entity. It is configured using the **19.17.53 ip-address** command.
Email	Email address. It is configured using the **19.17.44 email** command.
Serial-number	Serial number of the entity. It is configured using the **19.17.117 serial-number** command.

Related Topics

19.17.79 pki entity
19.17.18 country (PKI entity view)
19.17.120 state (PKI entity view)
19.17.61 locality
19.17.67 organization
19.17.66 organization-unit
19.17.17 common-name
19.17.53 ip-address
19.17.52 fqdn
19.17.44 email
19.17.117 serial-number

19.17.36 display pki ocsp cache detail

Function

The **display pki ocsp cache detail** displays the detail information of the OCSP cache.

Format

display pki ocsp cache detail

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

You can run this command to view detail information of the OCSP cache.

Example

Display the detail information of the OCSP cache.

```
<Huawei> display pki ocsp cache detail
================================================
Cache Hash Status Info:
num_items             = 0
num_nodes             = 8
num_alloc_nodes       = 16
num_expands           = 0
num_expand_reallocs   = 0
num_contracts         = 0
num_contract_reallocs = 0
num_hash_calls        = 0
num_comp_calls        = 0
num_insert            = 0
num_replace           = 0
num_delete            = 0
num_no_delete         = 0
num_retrieve          = 0
num_retrieve_miss     = 0
num_hash_comps        = 0

Cache Hash Node Status Info:
node      0 ->   0
node      1 ->   0
node      2 ->   0
node      3 ->   0
node      4 ->   0
node      5 ->   0
node      6 ->   0
node      7 ->   0

Cache Hash Node Usage Status Info:
0 nodes used out of 8
0 items
================================================
```

Table 19-167 Description of the **display pki ocsp cache detail** command output

Item	Description
Cache Hash Status Info	Hash status of the OCSP cache.
num_items	Number of available hash elements.
num_nodes	Number of requested hash nodes.
num_alloc_nodes	Maximum number of hash nodes that can be expanded.
num_expands	Number of hash node expansion application times.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
num_expand_reallocs	Number of expanded hash nodes.
num_contracts	Number of hash node reduction times.
num_contract_reallocs	Number of reduced hash nodes.
num_hash_calls	Number of times the hash function is invoked.
num_comp_calls	Number of times the hash comparison function is invoked.
num_insert	Number of inserted hash nodes.
num_replace	Number of replaced hash nodes.
num_delete	Number of deleted hash nodes.
num_no_delete	Number of undeleted hash nodes.
num_retrieve	Number of times the hash nodes in the OCSP cache are matched.
num_retrieve_miss	Number of times the hash nodes in the OCSP cache are not matched.
num_hash_comps	Number of times the hash nodes in the OCSP cache are compared.
Cache Hash Node Status Info	Hash node status in the OCSP cache. For example, **node 0 -> 0** indicates that the number 0 node is unused; **node 0 -> 1** indicates that the number 0 node is in use.
Cache Hash Node Usage Status Info	Hash node use status in the OCSP cache.
n nodes used out of 8	There are 8 hash nodes, and n nodes are in use.
n items	The nth hash element.

19.17.37 display pki ocsp cache statistics

Function

The **display pki ocsp cache statistics** command displays statistics about cached OCSP responses.

Format

display pki ocsp cache statistics

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command shows statistics about cached OCSP responses, including the maximum number of OCSP responses that can be cached, cache update interval, and number of cached responses.

Example

Display statistics about cached OCSP responses.

```
<Huawei> display pki ocsp cache statistics

=====================================================
   OCSP Cache Function: Enable
   OCSP Cache Max Number: 2
   OCSP Cache Refresh Interval: 5 minutes
   OCSP Cache Current Number: 0
=====================================================
```

Table 19-168 Description of the **display pki ocsp cache statistics** command output

Item	Description
OCSP Cache Function	Whether OCSP caching is enabled. • Enable • Disable It is configured using the **19.17.100 pki ocsp response cache enable** command.
OCSP Cache Max Number	Maximum size of OCSP cache. It is configured using the **19.17.101 pki ocsp response cache number** command.
OCSP Cache Refresh Interval	OCSP cache update interval. It is configured using the **19.17.102 pki ocsp response cache refresh interval** command.
OCSP Cache Current Number	Number of cached OCSP responses.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.17.100 pki ocsp response cache enable
19.17.101 pki ocsp response cache number
19.17.102 pki ocsp response cache refresh interval

19.17.38 display pki ocsp server down-information

Function

The **display pki ocsp server down-information** command displays the DOWN state information of the OCSP server recorded on the device.

Format

display pki ocsp server down-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

There is a mechanism to determine whether the OCSP server is down. When the OCSP server corresponding to a URL cannot be accessed, the server status is set to DOWN. In this case, the device will not send OCSP requests to the URL for 10 minutes.

Example

Display the DOWN state information of the OCSP server.

```
<Huawei> display pki ocsp server down-information

=====================================================

 Server URL: http://10.1.1.1/ocsp
 Timeout Times: 1
 Last timeout until now: 5 seconds
=====================================================
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-169 Description of the **display pki ocsp server down-information** command output

Item	Description
Server URL	URL of an unreachable OCSP server. It is configured using the **19.17.64 ocsp url** command.
Timeout Times	Connection timeouts.
Last timeout until now	Time elapsed since the last connection timeout and now.

19.17.39 display pki peer-certificate

Function

The **display pki peer-certificate** command displays the imported certificates of the remote device.

Format

display pki peer-certificate { **name** *peer-name* | **all** }

Parameters

Parameter	Description	Value
name *peer-name*	Specifies the name of peer certificate.	The value must be an existing peer certificate file name.
all	Displays brief information about all certificates of the remote device.	-

Views

All views

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command shows information about imported certificates of the remote device, including signature algorithm, issuer, validity period, subject, public key, and PKI realm.

Example

Display brief information about all certificates of the remote device.

```
<Huawei> display pki peer-certificate all
  Peer certificate name :abcd
  Serial Number:
    12 19 3c d3 00 00 00 00 04 9a
  Subject:
    CN=a

Total Number: 1
```

Display detailed information about the certificate **abcd** of the remote device.

```
<Huawei> display pki peer-certificate name abcd
The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            12:19:3c:d3:00:00:00:00:04:9a
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=CA_ROOT
        Validity
            Not Before: Feb 19 13:00:22 2013 GMT
            Not After : Feb 19 13:10:22 2014 GMT
        Subject: CN=a
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (512 bit)
                Modulus:
                    00:b9:8b:47:65:a9:99:ed:58:b2:63:74:65:56:d1:
                    08:bb:1d:8f:4e:ed:72:a2:4a:ef:d8:45:3d:53:db:
                    c8:eb:df:53:9e:5f:c7:96:46:65:14:1a:ab:72:e9:
                    a2:71:c8:7a:f0:51:0c:cc:39:bb:14:75:7d:f1:bc:
                    88:2c:a7:2e:e9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                E2:5B:8A:03:58:01:C8:E3:14:BC:18:5B:F9:BD:00:68:5B:D1:90:4E
            X509v3 Authority Key Identifier:
                keyid:CE:BA:CA:39:C7:AD:6A:CB:85:17:D0:8A:8E:28:02:0B:52:D4:D9:2
B

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://10.1.1.1:8080/CertEnroll/CA_ROOT.crl

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=CA_ROOT,CN=AIA,CN=Public%20Key%20Ser
vices,CN=Services,CN=Configuration,DC=esap,DC=com?cACertificate?base?objectClass
=certificationAuthority
                CA Issuers - URI:http://www.example.com/CertEnroll/www.example.c
om_CA_ROOT.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
    Signature Algorithm: sha1WithRSAEncryption
        bb:8b:77:af:ae:df:2e:0c:bd:7a:29:6e:76:23:ad:7d:69:6d:
```

 Copyright © Huawei Technologies Co., Ltd.

```
      0d:16:d9:18:82:ad:4f:52:b3:cd:1c:1a:fc:34:00:33:36:8d:
      47:2a:20:24:52:b7:02:75:cc:ab:3b:4c:f8:2a:a9:a9:4f:46:
      fb:c2:21:00:c1:b5:c2:67:0c:b1:99:2a:62:7b:71:4d:e7:c2:
      93:29:bb:ec:b1:e9:28:82:2f:77:61:ec:28:66:35:cb:5f:15:
      04:73:77:d8:26:91:7b:a2:56:74:51:33:0b:f1:04:28:24:b2:
      71:58:ad:5c:f8:96:17:0d:f7:b7:5f:4b:b9:ed:09:79:bc:54:
      21:c5:9b:90:f7:7b:21:aa:5a:aa:6f:51:e4:79:ce:b8:35:8b:
      19:90:51:94:e6:c2:61:f8:24:46:85:4c:a9:69:bd:8a:ef:c2:
      64:b8:19:ab:0b:6b:ec:34:41:8d:43:43:44:d1:1b:4c:4a:23:
      cd:40:52:7a:2e:8c:5d:b6:62:55:93:45:c8:3e:de:b1:51:82:
      d0:bb:7c:b8:09:7b:97:08:7b:93:17:40:a8:6f:2d:ed:f4:3e:
      36:10:2a:20:e3:47:e1:fb:ad:fe:97:73:a7:53:d0:f8:52:ca:
      b6:0e:e8:f1:df:6c:7a:37:39:bb:82:f9:03:c9:4a:71:65:df:
      6f:37:e6:b7

Pki realm name: -
Certificate file name: -
Certificate peer name: abcd
```

Table 19-170 Description of the **display pki peer-certificate** command output

Item	Description
Peer certificate name	Peer certificate name.
The x509 object type is certificate	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.
Subject	Subject of the certificate.
Subject Public Key Info	Public key of the certificate.
Public Key Algorithm	Algorithm of the Public key.
Public-Key	Information about the RSA public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X509v3 certificate extensions.
X509v3 Subject Key Identifier	Identifier of a subject key.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
X509v3 CRL Distribution Points	CRL distribution points.
Full Name	Full name of CDP.
Authority Information Access	Authority information access.
Pki realm name	PKI realm name.
Certificate file name	Certificate file name.
Certificate peer name	Certificate peer name.

19.17.40 display pki realm

Function

The **display pki realm** command displays PKI realm information.

Format

display pki realm [*realm-name*]

Parameters

Parameter	Description	Value
realm-name	Displays the detailed information about a PKI realm. If the parameter is left blank, information about all PKI realms is displayed.	The PKI realm name must already exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command displays details about a PKI realm, including PKI realm name, associated CA, CA certificate subject name, URL of the certificate enrolled through SCEP, PKI entity name, digital fingerprint algorithm of CA certificate, and digital fingerprint of CA certificate.

Example

Display information about all PKI realms.

```
<Huawei> display pki realm abc
 Realm Name : abc
 CA ID: CA_ROOT
 CA Name: "/CN=ca_root"
 Enrollment URL: http://10.136.7.196:8080/certsrv/mscep/mscep.dll
 Certificate Request Interval(Minutes): 1
 Certificate Request Times: 5
 Enrollment Mode: RA
 Enrollment Method: SCEP
 Entity Name: abc
 CA Certificate Fingerprint Arithmetic: sha256
 CA Certificate Fingerprint: e71add0744360e91186b828412d279e06dcc15a4ab4bb3d1384
2820396b526a0
 OCSP Nonce: Enable
 OCSP URL: -
 Method for Getting CRL: HTTP
 CDP URL: -
 Certificate Revocation Check Method: -
 RSA Key Name: abc
 SM2 Key Name:
 Auto-enroll: Enable
 Auto-enroll Percent: 100%
 Auto-enroll Regenerate: Enable
 Auto-enroll Regenerate Key-size: 2048
 Auto-enroll Updated-effective: Disable
 Password Cipher: Enable
 Password: %^%#:,3/YY@~[@(`1DBbZ&o$s`B\@S+3:UT0tF9EzSM:%^%#
 Crl Update-period(Hours): 8
 Crl Cache: Enable
 Key-usage: -
 Vpn-instance: -
 Source Interface: -
 Enrollment-request Signature Message-digest-method: SHA256

 Total Number: 1
```

Table 19-171 Description of the **display pki realm** command output

Item	Description
Realm Name	PKI realm name. It is configured using the **19.17.103 pki realm (system view)** command.
CA ID	ID of the CA associated with the PKI realm.
CA Name	Subject name of a CA certificate.
Enrollment URL	URL of the certificate enrolled on the SCEP server. It is configured using the **19.17.48 enrollment-url** command.
Certificate Request Interval(Minutes)	Interval between two certificate enrollment status queries.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Certificate Request Times	Maximum number of certificate enrollment status queries.
Enrollment Mode	Certificate enrollment mode (whether enrolled through RA). It is configured using the **19.17.48 enrollment-url** command.
Enrollment Method	Certificate enrollment method, including: • SCEP: obtains certificate from CA using the SCEP protocol. • Self-Signed: obtains certificate using self-signature.
Entity Name	PKI entity name. It is configured using the **19.17.49 entity** command.
CA Certificate Fingerprint Arithmetic	Fingerprint algorithm of the CA certificate. It is configured using the **19.17.51 fingerprint** command.
CA Certificate Fingerprint	Digital fingerprint of the CA certificate. It is configured using the **19.17.51 fingerprint** command.
OCSP Nonce	Whether a nonce extension is added to the OCSP request sent by a PKI entity. • Enable: A nonce extension is added to the OCSP request sent by a PKI entity. • Disable: A nonce extension is not added to the OCSP request sent by a PKI entity. It is configured using the **19.17.62 ocsp nonce enable** command.
OCSP URL	OCSP server's URL. It is configured using the **19.17.64 ocsp url** command.
Method for Getting CRL	Method of obtaining CRL. • SCEP: updates the CRL automatically using SCEP. It is configured using the **19.17.23 crl scep** command. • HTTP: updates the CRL automatically using HTTP. It is configured using the **19.17.21 crl http** command. • LDAP: updates the CRL automatically using LDAP. It is configured using the **19.17.22 crl ldap** command.
CDP URL	URL of the CDP. It is configured using the **19.17.4 cdp-url** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Crl Cache	Whether the PKI realm is allowed to use the CRL in cache. • Enable: The PKI realm is allowed to use the CRL in cache. • Disable: The PKI realm is not allowed to use the CRL in cache. To configure whether to allow the PKI realm to use the CRL in cache, run the **19.17.20 crl cache** command.
Certificate Revocation Check Method	Certificate status check method. It is configured using the **19.17.5 certificate-check** command.
RSA Key Name	RSA key. It is configured using the **19.17.116 rsa local-key-pair** command.
SM2 Key Name	SM2 key.
Auto-enroll	Whether automatic certificate enrollment is enabled. • Enable: Automatic certificate enrollment is enabled. • Disable: Automatic certificate enrollment is disabled. It is configured using the **19.17.1 auto-enroll** command.
Auto-enroll Percent	The percentage of the certificate's validity period. It is configured using the **19.17.1 auto-enroll** command.
Auto-enroll Regenerate	Whether the RSA key pair will be generated during certificate updates. • Enable: The RSA key pair will be generated during certificate updates. • Disable: The RSA key pair will not be generated during certificate updates. It is configured using the **19.17.1 auto-enroll** command.
Auto-enroll Regenerate Key-size	RSA key length. It is configured using the **19.17.1 auto-enroll** command.
Auto-enroll Updated-effective	Whether the certificate takes effect immediately after being updated. • Enable: The certificate takes effect immediately after being updated. • Disable: The certificate does not take effect immediately after being updated. It is configured using the **19.17.1 auto-enroll** command.
Password Cipher	Whether the challenge password can be used. • Enable: The challenge password can be used. • Disable: The challenge password cannot be used.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Password	Password used to apply for or revoke a certificate. It is configured using the **19.17.68 password (PKI realm view)** command.
Crl Update-period(Hours)	CRL update interval. It is configured using the **19.17.24 crl update-period** command.
Key-usage	Purpose information carried in a certificate request packet. It is configured using the **19.17.54 key-usage** command.
Vpn-instance	VPN to which the PKI realm is added. It is configured using the **19.17.123 vpn-instance** command.
Source Interface	Source interface used by the device to communicate with the PKI server. It is configured using the **19.17.119 source interface** command.
Enrollment-request Signature Message-digest-method	Digest method used for the enrollment request packet of signed certificate. It is configured using the **19.17.47 enrollment-request signature message-digest-method** command.

19.17.41 display pki rsa built-in-ca public

Function

The **display pki rsa built-in-ca public** command displays RSA key pairs and public keys of the SSL decryption certificates.

Format

display pki rsa built-in-ca [**name** *key-name*] **public**

Parameters

Parameter	Description	Value
name *key-name*	Specifies the name of the RSA key pair that you want to view. If the *key-name* parameter is not specified, information about all RSA key pairs and public keys of SSL encryption certificate is displayed.	The value must be an existing RSA key pair name.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command shows information about the RSA key pairs and public keys of the SSL decryption certificates, including the creation time, key pair name, whether the key can be exported, and public key information.

Example

Display all RSA key pairs of the SSL decryption certificates.

```
<Huawei> display pki rsa built-in-ca public

=====================================================
Time of Key pair created: 11:29:55  2015/10/21
Key Name: rsakey
Key Index: 0
Key Modules: 2048 bit
Key Exportable: Yes
=====================================================
Key code:
30820109
  02820100
    EC4E155D 90CBE9A0 E9CBB6CD 42797C2D 6B4EC67C
    BCC48F5E CB04127B 1D11D113 EA38D620 4F7E1ABE
    D35A23CF E737A04B 6D2850B7 9388353B 5CBE0206
    B731048C CEC2B347 DA123971 169086B1 85AC3BD3
    21F5125B 4207EBF6 6A578ED5 B964C9BC E0C9B8DF
    083F2689 083966CF 3E577C36 41585C30 AD2A8AC0
    54773A1F 81B893D1 A2F846C9 609434F0 DE0F9412
    B9E803DB 4D7EFE4D C1564AEF 033ACE5A 15B7EF8A
    40401769 ACF3BB72 9D39AFFA 2ACC25E1 F020998F
    43B6FF3B 96126EA5 0FA978BD 4E8ECD5C B7CA1D34
    3D783C77 73AF8FC2 277911D0 DBA7A478 30441972
    8F247DF2 D5AB6085 A6661FEA A978100C 9B0D96E5
    482420D0 D7E83F54 FD4D735F 1B4A359B
  0203
    010001
```

Table 19-172 Description of the **display pki rsa built-in-ca public** command output

Item	Description
Time of Key pair created	Time when an RSA key pair is created.
Key Name	Name of an RSA key pair. It can be configured using the **19.17.105 pki rsa built-in-ca** command.
Key Index	Index of an RSA key pair.
Key Modules	Number of bits in an RSA key pair. It can be configured using the **19.17.105 pki rsa built-in-ca** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Key Exportable	Whether an RSA key pair can be exported. It can be configured using the **19.17.105 pki rsa built-in-ca** command.
Key code	Public key in an RSA key pair.

Related Topics

19.17.105 pki rsa built-in-ca

19.17.42 display pki rsa local-key-pair

Function

The **display pki rsa local-key-pair** command displays the public key in the RSA key pair.

Format

display pki rsa local-key-pair { **pem** | **pkcs12** } *filename* [**password** *password*]

display pki rsa local-key-pair [**name** *key-name*] **public** [**temporary**]

Parameters

Parameter	Description	Value
pem	Indicates that the file format is PEM.	-
pkcs12	Indicates that the file format is PKCS12.	-
filename	Specifies the name of the file that contains the RSA key pair.	The file name must already exist.
password *password*	Specifies the decryption password of RSA key pair. The value must be the same as the password set by **19.17.83 pki export rsa-key-pair**.	The value must be the name of an existing decryption password of the RSA key pair.
name *key-name*	Specifies the RSA key pair name.	The RSA key pair name must already exist.
temporary	Displays information about the RSA key pair saved in the temporary zone.	-

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command shows information about the RSA key pair and public key, including key pair creation time, key pair name, whether the key can be exported, and public key information.

If *key-name* is not specified, all RSA key pairs and public keys are displayed. If *key-name* is specified, the specified RSA key pair and public key are displayed.

Example

Display information about all RSA key pairs.

```
<Huawei> display pki rsa local-key-pair public

=====================================================
Time of Key pair created: 17:43:42  2016/4/18
Key Name: abc
Key Index: 0
Key Modules: 2048 bit
Key Exportable: Yes
Key Type: RSA signature key
=====================================================
Key code:
30820109
  02820100
    C23344E1 B2C2D653 EB134011 9266C6CC 7C18C45F
    440AF31F 98B29D4C D436757B F6785BB5 09EFA2A1
    09FDBB24 62F1914D 4F10678F 3BE8E3C0 E6F02FC9
    AFE2ADDE 98E07D2C A5732288 A5280D2B 6A785F59
    A8D19D37 9B80F7EF 1B15FB77 BD9C54D0 01AF270F
    90258F65 1A631282 50002C4F 23EF0482 1F62E356
    AC700041 B31AB3B4 5C7EB4C0 AFF2E5AF 3DDA4F4E
    F5B86502 08BA7AFE 37204C67 7149AE52 1462F25E
    16B777E8 E71BCFBE 0E9E02A7 C5FE6120 304BE6C3
    CEB2575A EA24EBB6 BA420994 C50F3662 D8F24F25
    0D833865 5A127754 2E954F7F 16292DAA AF9D2371
    E669ADFF 4EA9FFF8 CE8488D7 344EBCEB AAA74116
    B30EF506 C64A726E B1013CB4 E8FA6707
  0203
    010001
```

Table 19-173 Description of the **display pki rsa local-key-pair** command output

Item	Description
Time of Key pair created	Time when the RSA key pair is created.
Key Name	Name of a key pair. It is configured using the **19.17.106 pki rsa local-key-pair create** command.
Key Index	Index of the key.
Key Modules	Number of bits of the key.
Key Exportable	Whether the key can be exported.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Key Type	Type of the key.
Key code	Public key in the RSA key pair.

19.17.43 display pki sm2 local-key-pair public (System view)

Function

The **display pki sm2 local-key-pair public** command displays information about the SM2 key pair and public key.

Format

display pki sm2 local-key-pair [**name** *key-name*] **public**

Parameters

Parameter	Description	Value
name *key-name*	Specifies the name of the SM2 key pair that you want to view.	The value must be an existing SM2 key pair name.

Views

System view

Default Level

3: Management level

Usage Guidelines

This command shows information about the SM2 key pairs and public keys, including the creation time, key pair name, whether the key can be exported, and public key information.

If the *key-name* parameter is not specified, information about all SM2 keys and public keys is displayed. If the *key-name* parameter is specified, information about only the specified SM2 key and public key is displayed.

Example

Display information about all SM2 key pairs.

```
<Huawei> display pki sm2 local-key-pair public

=====================================================
Time of Key pair created: 16:59:08  2016/4/15
```

 Copyright © Huawei Technologies Co., Ltd.

```
Key Name: 123
Key Index: 0
Key Modules: -
Key Exportable: No
=====================================================
Public-Key: (256 bit)
pub:
    04:d8:bc:77:f6:cd:6d:65:5f:c2:08:29:a4:ad:de:
    bf:d6:ee:59:5e:ba:a1:e2:38:6f:d5:e4:ff:4c:a3:
    97:b2:3b:1a:1d:12:02:5a:5d:a2:57:21:6a:8e:e5:
    29:3d:5f:84:b6:5a:5f:b9:5f:f4:76:f8:26:34:fb:
    ea:f0:66:b9:eb
Field Type: prime-field
Prime:
    00:ff:ff:ff:fe:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:
    ff:ff:ff
A:
    00:ff:ff:ff:fe:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:
    ff:ff:fc
B:
    28:e9:fa:9e:9d:9f:5e:34:4d:5a:9e:4b:cf:65:09:
    a7:f3:97:89:f5:15:ab:8f:92:dd:bc:bd:41:4d:94:
    0e:93
Generator (uncompressed):
    04:32:c4:ae:2c:1f:19:81:19:5f:99:04:46:6a:39:
    c9:94:8f:e3:0b:bf:f2:66:0b:e1:71:5a:45:89:33:
    4c:74:c7:bc:37:36:a2:f4:f6:77:9c:59:bd:ce:e3:
    6b:69:21:53:d0:a9:87:7c:c6:2a:47:40:02:df:32:
    e5:21:39:f0:a0
Order:
    00:ff:ff:ff:fe:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:72:03:df:6b:21:c6:05:2b:53:bb:f4:09:39:
    d5:41:23
Cofactor:  1 (0x1)
```

Table 19-174 Description of the **display pki sm2 local-key-pair public** command output

Item	Description
Time of Key pair created	SM2 Key pair creation time.
Key Name	Name of the SM2 key pair.
Key Index	SM2 Key index.
Key Modules	SM2 Key modules.
Key Exportable	Whether the SM2 key can be exported.
Public-Key	SM2 Public key information.
pub	Public key in the SM2 key pair.
A	Prime number a in the SM2 elliptic curve cryptography (ECC).
B	Prime number b in the SM2 ECC.
Generator (uncompressed)	Generator of the SM2 ECC and whether the generator is compressed if it is converted into a large value.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Order	Order of the SM2 ECC generator.
Cofactor	Cofactor of the SM2 ECC, which is the Number of ECC points/Order of generator.

19.17.44 email

Function

The **email** command configures an email address for a PKI entity.

The **undo email** command cancels the configuration.

By default, no email address for an entity is configured.

Format

email *email-address*

undo email

Parameters

Parameter	Description	Value
email-address	Specifies the email address of an entity.	The value is a string of 1 to 128 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), underscores (_), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an email address for the PKI entity, which is used as an alias of the entity.

After the email address is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this email address. The CA server

 Copyright © Huawei Technologies Co., Ltd.

verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the email address of the PKI entity.

Example

Set the email address to test@example.com for an entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] email test@example.com
```

Related Topics

19.17.35 display pki entity

19.17.45 enrollment self-signed

Function

The **enrollment self-signed** command configures self-signed certificate obtaining in the PKI realm.

The **undo enrollment self-signed** command restores the default certificate obtaining method.

By default, self-signed certificate obtaining in the PKI realm is not configured.

Format

enrollment self-signed

undo enrollment self-signed

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **enrollment self-signed** command configures self-signed certificate obtaining in the PKI realm. The device can use the self-signed certificate obtained from the PKI realm to support default HTTPS functions.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The RSA key pair has been configured by using the **19.17.116 rsa local-key-pair** command.

Precautions

The device generates a self-signed certificate only when the PKI domain is applied to the service.

The device does not support lifecycle management for self-signed certificates. For example, self-signed certificates cannot be registered, updated, or revoked on the device. To ensure security of the device and certificates, it is recommended the user's certificate be used.

To configure self-signed certificate obtaining, delete the certificate in the PKI realm.

After the **enrollment self-signed** command is run, the device will not generate certificate expiration logs when its self-signed certificate expires.

Example

Configure self-signed certificate obtaining in the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] enrollment self-signed
```

Related Topics

19.17.103 pki realm (system view)

19.17.40 display pki realm

19.17.46 enrollment-request specific

Function

The **enrollment-request specific** command configures the device to use a certificate request packet of the specific format to apply for a local certificate from the CA.

The **undo enrollment-request specific** command restores the default setting.

By default, the device uses a certificate request packet of the standard format to apply for a local certificate from the CA.

Format

enrollment-request specific

undo enrollment-request specific

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to configure this command to implement communication between the PKI entity and the CA server when the CA server has the following requirements:

- The unstructured address and unstructured name of the certificate request packet do not carry the SET identifier.
- The device uses the private key of the applied certificate to sign the certificate request packet.

Precautions

To implement communication between the device and CA server, the certificate key length cannot be longer than 2048 bits. If the RSA key length of certificates is longer than 2048 bits, the device will use the private key of a self-signed certificate to sign the certificate request packet regardless of whether the **enrollment-request specific** command is configured.

Example

Configure the device to use a certificate request packet of the specific format to apply for a local certificate from the CA.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] enrollment-request specific
```

19.17.47 enrollment-request signature message-digest-method

Function

The **enrollment-request signature message-digest-method** command sets the message digest method of signature for the enrollment request.

The **undo enrollment-request signature message-digest-method** command restores the default message digest method.

By default, the message digest method of signature for the enrollment request is **sha-256**.

Format

enrollment-request signature message-digest-method { **md5** | **sha1** | **sha-256** | **sha-384** | **sha-512** }

undo enrollment-request signature message-digest-method

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
md5	Sets the digest method used for the enrollment request packet of signed certificate to MD5.	-
sha1	Sets the digest method used for the enrollment request packet of signed certificate to SHA1.	-
sha-256	Sets the digest method used for the enrollment request packet of signed certificate to SHA2-256.	-
sha-384	Sets the digest method used for the enrollment request packet of signed certificate to SHA2-384.	-
sha-512	Sets the digest method used for the enrollment request packet of signed certificate to SHA2-512.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

In SCEP local certificate application mode, after a CA server receives a certificate enrollment request from a PKI entity, the CA server requests a signature for authentication, and generates a local certificate only after the authentication is successful.

Other algorithms are more secure than MD5 and SHA1 algorithms and so are recommended.

Example

Set the message-digest method of signature for enrollment request to be **sha-384**.

```
<Huawei> system-view
[Huawei] pki realm e
[Huawei-pki-realm-e] enrollment-request signature message-digest-method sha-384
```

19.17.48 enrollment-url

Function

The **enrollment-url** command configures the URL of the CA server.

The **undo enrollment-url** command deletes the URL of the CA server.

By default, the URL of the CA server is not configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

enrollment-url [**esc**] *url* [**interval** *minutes*] [**times** *count*] [**ra**]

undo enrollment-url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url	Specifies the URL of the CA server. The URL is in the format of *http://server_location/ca_script_location*. *server_location* can use only the IP address format and domain name resolution. *ca_script_location* is the path where CA's application script is located. For example, **http://10.1.1.1:8080/certsrv/mscep/mscep.dll**.	The value is a string that starts with **http://** and consists of 1 to 128 case-sensitive characters without spaces.
interval *minutes*	Specifies the interval between two certificate enrollment status queries.	The value is an integer that ranges from 1 to 1440, in minutes. The default value is 1.
times *count*	Specifies the maximum number of certificate enrollment status queries.	The value is an integer that ranges from 1 to 100. The default value is 5.
ra	Configures an RA to authenticate a PKI entity's identity information during local certificate application. By default, a CA authenticates a PKI entity's identity information during local certificate application.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The URL refers to the address provided by a CA server for certificate application. For example, a CA server running Windows Server 2008 uses a URL address in the format http://host:port/certsrv/mscep/mscep.dll, in which *host* indicates the IP address of the CA server and *port* indicates the port number.

The keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

Create a PKI realm **test** and configure the URL of the CA server.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] enrollment-url http://10.1.1.1:8080/certsrv/mscep/mscep.dll ra
```

19.17.49 entity

Function

The **entity** command specifies a PKI entity that applies for a certificate.

The **undo entity** command cancels a PKI entity.

By default, no PKI entity is specified.

Format

entity *entity-name*

undo entity

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity.	The value must be an existing PKI entity name.

 Copyright © Huawei Technologies Co., Ltd.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PKI entity requests the local certificate in the PKI realm, the device encapsulates the configuration of the specified PKI entity into the certificate request.

Prerequisites

1. The specified PKI entity has been configured by using the **19.17.79 pki entity** command.
2. The common name of the PKI entity has been configured using the **19.17.17 common-name** command.

Precautions

A PKI realm can be bound to only one PKI entity.

Example

Bind the PKI entity **a** to the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki entity a
[Huawei-pki-entity-a] common-name test
[Huawei-pki-entity-a] quit
[Huawei] pki realm abc
[Huawei-pki-realm-abc] entity a
```

Related Topics

19.17.79 pki entity

19.17.17 common-name

19.17.40 display pki realm

19.17.50 extension-request enterprise

Function

The **extension-request enterprise** command configures the extended attribute in the certificate enrollment request to carry the object ID defined by Verisign.

The **undo extension-request enterprise** command restores the default extended attribute in the certificate enrollment request.

By default, the extended attribute in the certificate enrollment request carries the object ID defined by PKCS#9.

 Copyright © Huawei Technologies Co., Ltd.

Format

extension-request enterprise verisign

undo extension-request enterprise verisign

Parameters

Parameter	Description	Value
verisign	Inserts the object ID defined by Verisign into the extended attribute of the certificate enrollment request.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

When a PKI entity applies for a local certificate from the CA, the certificate applicant requires that the extended attribute in the local certificate carry the object ID defined by Verisign. You can run this command.

Example

Configure the extended request attribute in the certificate enrollment request to carry the object ID defined by Verisign.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] extension-request enterprise verisign
```

19.17.51 fingerprint

Function

The **fingerprint** command configures the CA certificate fingerprint used in CA certificate authentication.

The **undo fingerprint** command deletes the CA certificate fingerprint used in CA certificate authentication.

By default, no CA certificate fingerprint is configured for CA certificate authentication.

Format

fingerprint { **md5** | **sha1** | **sha256** } *fingerprint*

undo fingerprint

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
md5	Sets the digital fingerprint algorithm to MD5.	-
sha1	Sets the digital fingerprint algorithm to SHA1.	-
sha256	Sets the digital fingerprint algorithm to SHA256.	-
fingerprint	Specifies the digital fingerprint value. This value needs to be obtained from the CA server offline. For example, from a CA server running Windows Server 2008, you can obtain the digital fingerprint at http://*host*:*port*/certsrv/mscep_admin/, in which *host* indicates the server's IP address and *port* indicates the port number.	The digital fingerprint value is a hexadecimal string of case-insensitive characters. ● An MD5 fingerprint consists of 32 characters (16 bytes). ● An SHA1 fingerprint consists of 40 characters (20 bytes). ● An SHA256 fingerprint consists of 64 characters (32 bytes).

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When obtaining a CA certificate, the device uses an algorithm to calculate the CA certificate fingerprint and compares the CA certificate fingerprint with the configured fingerprint. If the two values are the same, the device receives the CA certificate. When verifying a certificate, the device uses the public key of the CA certificate to authenticate the digital signature. If the digital signature can be decrypted, the certificate is verified.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

You can configure an algorithm to calculate the CA certificate fingerprint. If you run the **fingerprint** command multiple times in the same PKI realm view, only the latest configuration takes effect.

The MD5 and SHA1 algorithms have a low security level. SHA256 is recommended.

Example

Configure the CA certificate fingerprint used in CA certificate authentication.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] fingerprint sha256
e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0
```

19.17.52 fqdn

Function

The **fqdn** command configures a fully qualified domain name (FQDN) for an entity.

The **undo fqdn** command cancels the configuration.

By default, no FQDN is configured for a PKI entity.

Format

fqdn [**unstructed-name**] *fqdn-name*

undo fqdn [**unstructed-name**]

Parameters

Parameter	Description	Value
unstructed-name	Indicates that FQDN is used as the PKCS#9 unstructed name for the PKI entity. If this parameter is not specified, FQDN is used as the alias of the PKI entity.	-
fqdn-name	Specifies the FQDN of an entity.	The value is a string of 1 to 255 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), underscores (_), and spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an FQDN for the PKI entity, which is used as an alias of the entity.

An FQDN is the unique identifier of a PKI entity. It consists of a host name and a domain name, and can be translated into an IP address. A sample of an FQDN is www.example.com.

After the FQDN is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this FQDN. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the FQDN of the PKI entity.

If the **enrollment-request specific** command has been executed to configure the PKI entity to apply for a local certificate from the CA using the specified enrollment request format, the **unstructed-name** parameter can be specified to configure FQDN as the PKCS#9 unstructed name for the PKI entity.

Example

Set the FQDN to **example.com** for an entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] fqdn example.com
```

Related Topics

19.17.35 display pki entity

19.17.53 ip-address

Function

The **ip-address** configures an IP address for an entity.

The **undo ip-address** deletes the configuration.

By default, a PKI entity does not have an IP address.

Format

ip-address [**unstructed-address**] { *ipv4-address* | *interface-type interface-number* }

 Copyright © Huawei Technologies Co., Ltd.

undo ip-address [**unstructed-address**]

Parameters

Parameter	Description	Value
unstructed-address	Indicates that an IP address is used as the PKCS#9 unstructed address for the PKI entity. If this parameter is not specified, an IP address is used as the alias of the PKI entity.	-
ipv4-address	Specifies the IPv4 address of a PKI entity.	The value is in dotted decimal notation.
interface-type interface-number	Specifies an interface IP address of a PKI entity. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity include the identity information of the PKI entity. The CA identifies a certificate applicant based on identity information provided by a PKI entity. To facilitate applicant identification, configure an IP address for the PKI entity, which is used as an alias of the PKI entity.

After an IP address is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this IP address. After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the device IP address.

If the **enrollment-request specific** command has been executed to configure the PKI entity to apply for a local certificate from the CA using the specified enrollment request format, the **unstructed-name** parameter can be specified to configure IP address as the PKCS#9 unstructed address for the PKI entity.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the IP address for a PKI entity to 10.1.1.1.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] ip-address 10.1.1.1
```

Related Topics

19.17.35 display pki entity

19.17.54 key-usage

Function

The **key-usage** command configures the purpose description for a certificate public key.

The **undo key-usage** command deletes the purpose description of a certificate public key.

By default, a certificate public key does not have a purpose description.

Format

key-usage { **ike** | **ssl-client** | **ssl-server** } *

undo key-usage { **ike** | **ssl-client** | **ssl-server** } *

Parameters

Parameter	Description	Value
ike	Specifies the usage of a key as ike. That is, the key is used to set up an IPSec tunnel.	-
ssl-client	Specifies the usage of a key as ssl-client. That is, the key is used by the SSL client to set up an SSL session.	-
ssl-server	Specifies the usage of a key as ssl-server. That is, the key is used by the SSL server to set up an SSL session.	-

Views

PKI realm view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To improve certificate security, you can add the usage information of a key to the certificate request packet sent from the device to the CA server.

After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the usage information of the key.

For example, when setting up an SSL session, the SSL client adds a digital signature and encrypts the key by using the certificate. After you specify the usage of a key as ssl-client by using the **key-usage ssl-client** command, the certificate generated by the CA server carries the usage information, including a digital signature and encrypted key. If you use this key to encrypt data, the key will be invalid.

Example

Specify the usage of a key as ssl-client.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] key-usage ssl-client
```

19.17.55 ldap-server authentication

Function

The **ldap-server authentication** command configures an LDAP authentication server.

The **undo ldap-server authentication** command deletes an LDAP authentication server.

By default, no LDAP authentication server is configured.

Format

ldap-server authentication *ip-address* [*port-number*]

undo ldap-server authentication

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an LDAP authentication server.	The value is in dotted decimal notation.
port-number	Specifies the port number of an LDAP authentication server.	The value is an integer that ranges from 1 to 65535. The default value is 389. The port number must be the same as that on the LDAP server.

 Copyright © Huawei Technologies Co., Ltd.

Views

LDAP server template view

Default Level

3: Management level

Usage Guidelines

During LDAP authentication, LDAP is used in interaction between the device and LDAP server. The LDAP data transmission is not encrypted. For security, you can use LDAP based on SSL for encrypted transmission. LDAP server certificates need to be imported into the device to authenticate the LDAP server.

Example

Configure the primary LDAP authentication server.

```
<Huawei> system-view
[Huawei] ldap-server template temp1
[Huawei-ldap-temp1] ldap-server authentication 10.1.1.1 389
```

19.17.56 ldap-server authentication manager

Function

The **ldap-server authentication manager** command configures the administrator DN and password of an LDAP authentication server.

The **undo ldap-server authentication manager** command deletes the values of the administrator DN and password of an LDAP authentication server.

By default, no administrator DN and password of an LDAP authentication server is configured.

Format

ldap-server authentication manager *manager-dn* [*password* [*repassword*]]

undo ldap-server authentication manager

Parameters

Parameter	Description	Value
manager-dn	Specifies the administrator DN of an LDAP authentication server.	If the *manager-dn* value does not contain any space, its length ranges from 1 to 256.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password	Specifies the administrator password of an LDAP authentication server.	The value is a string that contains 1 to 63 characters in simple text or 48 to 108 characters in cipher text. The simple characters are saved in cipher text. If the string has 1 to 16 characters, the cipher text is 48-byte long; if the string has 17 to 32 characters, the cipher text is 68-byte long; if the string has 33 to 48 characters, the cipher text is 88-byte long; if the string has 49 to 63 characters, the cipher text is 108-byte long. **NOTICE** To enhance security, the password of an LDAP administrator is recommended to meet the minimum strength requirements, that is, it needs to contain at least three types of the following characters: upper-case letters, lower-case letters, digits (0 to 9), and special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%), and contains at least six characters.
repassword	Re-enters the password of an LDAP administrator.	The value must be the same as that of *password*.

Views

LDAP server template view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Set the administrator DN and password of an LDAP authentication server to **dn** and **Admin@123**, respectively.

```
<Huawei> system-view
[Huawei] ldap-server template temp1
[Huawei-ldap-temp1] ldap-server authentication manager dn Admin@123
```

19.17.57 ldap-server authentication manager-password

Function

The **ldap-server authentication manager-password** command modifies the administrator password of an LDAP authentication server.

Format

ldap-server authentication manager-password *password* [*repassword*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
password	Specifies the administrator password of an LDAP authentication server.	The value is a string that contains 1 to 63 characters in simple text or 48 to 108 characters in cipher text. The simple characters are saved in cipher text. If the string has 1 to 16 characters, the cipher text is 48-byte long; if the string has 17 to 32 characters, the cipher text is 68-byte long; if the string has 33 to 48 characters, the cipher text is 88-byte long; if the string has 49 to 63 characters, the cipher text is 108-byte long. **NOTICE** To enhance security, the password of an LDAP administrator is recommended to meet the minimum strength requirements, that is, it needs to contain at least three types of the following characters: upper-case letters, lower-case letters, digits (0 to 9), and special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%), and contains at least six characters.
repassword	Re-enters the password of an LDAP administrator.	The value must be the same as that of *password*.

Views

LDAP server template view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Set the administrator password of an LDAP authentication server to **Admin@123** respectively.

```
<Huawei> system-view
[Huawei] ldap-server template temp1
[Huawei-ldap-temp1] ldap-server authentication manager-password Admin@123
```

19.17.58 ldap-server template

Function

The **ldap-server template** command creates an LDAP server template and displays the LDAP server template view.

The **undo ldap-server template** command deletes an LDAP server template.

By default, no LDAP server template is configured.

Format

ldap-server template *template-name*

undo ldap-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an LDAP server template.	The value is a case-sensitive string of 1 to 32 characters. The name contains only uppercase letters, lowercase letters, digits, dots (.), underscores (_), hyphens (-) and their combinations.

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If an LDAP server template is referenced by an authentication domain, you can modify the LDAP server template, but cannot delete it.

If you attempt to delete an LDAP template in use, the system prompts the deletion failure.

Example

Create an LDAP server template named **temp1** and access the corresponding view.

```
<Huawei> system-view
[Huawei] ldap-server template temp1
[Huawei-ldap-temp1]
```

19.17.59 ldap-server-template

Function

The **ldap-server-template** command specifies a LDAP server template for a PKI realm.

The **undo ldap-server-template** command deletes the LDAP server template from the PKI realm.

By default, no LDAP server template is configured in the PKI realm.

Format

ldap-server-template *template-name*

undo ldap-server-template

Parameters

Parameter	Description	Value
template-name	Specifies the name of an LDAP server template.	The LDAP server template name must already exist.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

This command is required when LDAP is selected for certificate download or automatic CRL update.

Prerequisites

1. An LDAP server template has been created using the **19.17.58 ldap-server template** command.
2. Automatic CRL update mode is set to LDAP using the **19.17.22 crl ldap** command.

Example

Specify an LDAP server template for a PKI realm.

```
<Huawei> system-view
[Huawei] ldap-server template user1
[Huawei-ldap-user1] quit
[Huawei] pki realm abc
[Huawei-pki-realm-abc] crl ldap
[Huawei-pki-realm-abc] ldap-server-template user1
```

Related Topics

19.17.58 ldap-server template

19.17.22 crl ldap

19.17.60 ldap-server (PKI realm view)

Function

The **ldap-server** command configures an LDAP server.

The **undo ldap-server** command cancels the configuration.

By default, no LDAP server is configured.

Format

ldap-server { **authentication** *ldap-dn ldap-password* | **ip** *ip-address* [**port** *port* | **version** *version*] * }

undo ldap-server [**authentication**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
authentication *ldap-dn ldap-password*	Indicates the user name and password of an LDAP server.	• *ldap-dn*: The value is a string of 1 to 32 case-sensitive characters. • *ldap-password*: The value is a string of 1 to 32 case-sensitive characters without spaces or question marks. If the character string is quoted by double quotation marks, it can contain spaces and question marks. The system saves this string to the configuration file in ciphertext. A string of 1-16 characters is converted into a 48-byte cipher-text string; a string of 17-32 characters is converted into a 68-byte cipher-text string.
ip *ip-address*	Specifies the IP address of an LDAP server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of an LDAP server.	The value is an integer that ranges from 1 to 65535. The default value is 389.
version *version*	Specifies the version number of LDAP.	The value is an integer that ranges from 2 to 3. The default value is 3.

Views

PKI realm view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a PKI entity uses LDAP to update CRL for certificate verification, the PKI entity obtains CRL from the LDAP server. In this situation, you need to specify an LDAP server.

Prerequisites

The automatic CRL update mode is set to LDAP using the **crl ldap** command.

Example

Configure the IP address to 10.1.1.1, port number to 3389, and LDAP version number to 2 for an LDAP server.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl ldap
[Huawei-pki-realm-d1] ldap-server ip 10.1.1.1 port 3389 version 2
```

19.17.61 locality

Function

The **locality** command configures a locality name for a PKI entity.

The **undo locality** command cancels the configuration.

By default, a PKI entity does not have a locality name.

Format

locality *locality-name*

undo locality

Parameters

Parameter	Description	Value
locality-name	Specifies the locality name of an entity.	The value is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a locality name for the PKI entity, which is used as an alias of the entity.

After the locality name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this locality name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the locality name of the PKI entity.

Example

Set the locality name to **Beijing** for a PKI entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] locality Beijing
```

Related Topics

19.17.35 display pki entity

19.17.62 ocsp nonce enable

Function

The **ocsp nonce enable** command adds a nonce extension to the OCSP request sent by a PKI entity.

The **undo ocsp nonce enable** command cancels the configuration.

By default, the OCSP request sent by a PKI entity contains a nonce extension.

Format

ocsp nonce enable

undo ocsp nonce enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To improve security and reliability of communication between PKI entity and OCSP server, this command adds a nonce extension (a random value) to the OSCP request sent by the PKI entity. If the nonce extension values on the PKI entity and OCSP server are different, communication fails.

Example

Add a nonce extension to the OCSP request sent by a PKI entity

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] ocsp nonce enable
```

19.17.63 ocsp signature enable

Function

The **ocsp signature enable** command enables the function of signing OCSP request packets.

The **undo ocsp signature enable** command disables the function of signing OCSP request packets.

By default, the function of signing OCSP request packets is disabled.

Format

ocsp signature enable

undo ocsp signature enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

When the certificate check mode is set to OCSP, the device sends OCSP request packets to the OCSP server. To improve access security, run this command to enable signing on OCSP request packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] ocsp signature enable
```

19.17.64 ocsp url

Function

The **ocsp url** command configures the Uniform Resource Locator (URL) address for the Online Certificate Status Protocol (OCSP) server.

The **undo ocsp url** command deletes the URL address of the OCSP server.

By default, an OCSP server does not have a URL address.

Format

ocsp url [**esc**] *url-address*

undo ocsp url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url-address	Indicates the OCSP server's URL address.	The value is a string starting with **http://** and consisting of 1 to 128 case-sensitive characters without spaces.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

If a certificate to be checked through OCSP does not contain the AIA option, run this command to configure the OCSP server's URL. If the certificate contains the AIA option, run the **ocsp-url from-ca** command to configure the PKI entity to obtain OSCP server's URL from the AIA option.

Keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code, and **3f** is the hexadecimal ASCII code for the question mark (?).

 Copyright © Huawei Technologies Co., Ltd.

Therefore, the entered URL must be in **\x3f** format. For example, the URL that an administrator needs to enter is **http://www.***.com\x3fpage1**, instead of **http://www.***.com?page1**. If the administrator wants to configure **http://www.***com?page1\x3f** that includes both a question mark (?) and **\x3f**, the administrator should add an escape character (\) to \x3f and enter **http://www.***.com\x3fpage1\\x3f.**

Example

Set the OCSP server's URL address to http://10.1.1.1.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] ocsp url http://10.1.1.1
```

19.17.65 ocsp-url from-ca

Function

The **ocsp-url from-ca** command configures the PKI entity to obtain the OCSP server's URL from the Authority Info Access (AIA) option in the CA certificate.

The **undo ocsp-url from-ca** command disables the PKI entity from obtaining the OCSP server's URL from the Authority Info Access (AIA) option in the CA certificate.

By default, a PKI entity does not obtain OCSP server's URL from the CA certificate's AIA option.

Format

ocsp-url from-ca

undo ocsp-url from-ca

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

If a certificate to be checked through OCSP contains the AIA option, run this command to configure the PKI entity to obtain OSCP server's URL from the AIA option. If the certificate does not contain the AIA option, run the **ocsp url** command to configure the OCSP server's URL.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the PKI entity to obtain OCSP server's URL from the CA certificate's AIA option.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] ocsp-url from-ca
```

19.17.66 organization-unit

Function

The **organization-unit** command configures the department name for a PKI entity.

The **undo organization-unit** command restores the default setting.

By default, no department name is configured for a PKI entity.

Format

organization-unit *organization-unit-name*

undo organization-unit

Parameters

Parameter	Description	Value
organization-unit-name	Specifies the department name for a PKI entity.	The department name is a string of 1 to 31 case-sensitive characters. Names of departments are separated by commas (,). The total length of all department names ranges from 1 to 191. The characters can be letters, integers, apostrophe ('), equal sign (=), brackets (), plus sign (+), comma (,), minus sign (-), dot (.), slash (/), colon (:), and spaces.

Views

PKI entity view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a department name for the PKI entity, which is used as an alias of the entity.

After the department name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this department name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the department name of the PKI entity.

Example

Configure the department name of a PKI entity to **Group1, Sale**.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] organization-unit Group1,Sale
```

Related Topics

19.17.35 display pki entity

19.17.67 organization

Function

The **organization** command configures a PKI entity's organization name.

The **undo organization** command deletes a PKI entity's organization name.

By default, a PKI entity does not have an organization name.

Format

organization *organization-name*

undo organization

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
organization-name	Specifies the organization name of the PKI entity.	It is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an organization name for the PKI entity, which is used as an alias of the entity.

After the organization name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this organization name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the organization name of the PKI entity.

Example

Set the organization name of the PKI entity to **org1**.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] organization org1
```

Related Topics

19.17.35 display pki entity

19.17.68 password (PKI realm view)

Function

The **password** command sets the challenge password used for certificate application through SCEP, which is also used to revoke a certificate.

The **undo password** command deletes the challenge password used for certificate application through SCEP.

 Copyright © Huawei Technologies Co., Ltd.

By default, no challenge password is configured.

Format

password cipher *password*

undo password

Parameters

Parameter	Description	Value
cipher *password*	Specifies the challenge password used for certificate application through SCEP. The password is displayed in ciphertext.	The value is a string of case-sensitive characters. It cannot contain question marks (?). The *password* is in plaintext that contains 1 to 64 characters or in ciphertext that contains 48 to 108 characters. **NOTE** To improve communication security, it is recommended that the certificate revocation password contains at least three types of lowercase letters, uppercase letters, numerals, and special characters, and contains at least six characters.

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

When a PKI entity uses SCEP to apply for a certificate from CA, CA needs to verify the challenge password of the entity. CA accepts the certificate application request only when the challenge password is correct. You need to run this command to set a challenge password for the PKI entity.

The challenge password is also used to revoke a certificate. It avoids misoperations in certificate revocation.

Example

Set the challenge password used to apply for certificate through SCEP.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] password cipher 6AE73F21E6D3571D
```

19.17.69 pki built-in-ca match-rsa-key

Function

The **pki built-in-ca match-rsa-key** command configures a device to search for the RSA key pair associated with a specific SSL decryption certificate.

Format

pki built-in-ca match-rsa-key certificate-filename *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of an SSL decryption certificate.	It must be the name of an existing SSL decryption certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to view the RSA key pair associated with an SSL decryption certificate. Then the system searches all local RSA key pairs for the desired one, and displays the key pair name.

Prerequisites

An SSL decryption certificate has been generated using the **19.17.86 pki generate built-in-ca certificate** command or an SSL decryption certificate has been imported.

Example

Configure a device to search for the RSA key pair that matches certificate file **rsakey_builtinca.cer**.

```
<Huawei> system-view
[Huawei] pki generate built-in-ca certificate rsa-key-pair rsakey entity entity1
 Please enter the file name for built in CA certificate <length 1-64> : rsakey_builtinca.cer
 Info: Generate built in CA certificate successfully.
[Huawei] pki built-in-ca match-rsa-key certificate-filename rsakey_builtinca.cer
 Info: The file rsakey_builtinca.cer contains certificates 1.
 Info: Certificate 1 from file rsakey_builtinca.cer matches RSA key rsakey.
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.17.86 pki generate built-in-ca certificate

19.17.70 pki cmp certificate-request session

Function

The **pki cmp certificate-request session** command sends a certificate request (CR) to the CMPv2 server based on the CMP session information.

Format

pki cmp certificate-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of the CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device has a certificate issued by CA, the device can perform a CR to apply for a certificate for another device.

After this command is executed, the system checks whether the configurations in the CMP session is sufficient for certificate application. If no, the system displays an error message. If yes, the system performs the CR according to the configuration. The obtained certificate is saved in a file on the CF card or Hda1, but not imported to the memory.

NOTE

The device does not support the message authentication code mode. If the CMP session mode is set to message authentication code, the system displays an error message.

Prerequisites

A CMP session has been created using the **19.17.73 pki cmp session** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Send a CR to the CMPv2 server.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] quit
[Huawei] pki cmp certificate-request session test
 Info: Initializing configuration.
 Info: Creatting certification request packet.
 Info: Connectting to CMPv2 server.
 Info: Sending certification request packet.
 Info: Waitting for certification response packet.
 Info: Creatting confirm packet.
 Info: Connectting to CMPv2 server.
 Info: Sending confirm packet.
 Info: Waitting for confirm packet from server.
 Info: CMPv2 operation finish.
```

Related Topics

19.17.73 pki cmp session

19.17.71 pki cmp initial-request session

Function

The **pki cmp initial-request session** command performs an initial request (IR) to the CMPv2 server based on the CMP session information.

Format

pki cmp initial-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the command is executed, the system checks whether the configurations in the CMP session are sufficient for certificate application. If no, the system displays an error message. If yes, the system performs an IR according to the configuration.

 Copyright © Huawei Technologies Co., Ltd.

The obtained certificate is saved in a file on the CF card or Hda1, but not imported to the memory. If the server issues the CA certificate during the response period, the CA certificate is also saved in a file.

Prerequisites

A CMP session has been created using the **19.17.73 pki cmp session** command.

Example

Send an IR to the CMPv2 server.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] quit
[Huawei] pki cmp initial-request session test
 Info: Initializing configuration.
 Info: Creatting initial request packet.
 Info: Connectting to CMPv2 server.
 Info: Sending initial request packet.
 Info: Waitting for initial response packet.
 Info: Creatting confirm packet.
 Info: Connectting to CMPv2 server.
 Info: Sending confirm packet.
 Info: Waitting for confirm packet from server.
 Info: CMPv2 operation finish.
```

Related Topics

19.17.73 pki cmp session

19.17.72 pki cmp keyupdate-request session

Function

The **pki cmp keyupdate-request session** command performs a key update request (KUR) to the CMPv2 server based on the CMP session information.

Format

pki cmp keyupdate-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A device performs a KUR when it has a certificate issued by the CA and requires to update the certificate.

After the command is executed, the system checks whether the configurations in the CMP session are sufficient for certificate update application. If no, the system displays an error message. If yes, the system performs a KUR according to the configuration. The updated certificate is saved in a file on the device storage, but not imported to the memory.

NOTE

The device does not support the message authentication code mode. If the CMP session mode is set to message authentication code, the system displays an error message.

Prerequisites

A CMP session has been created using the **19.17.73 pki cmp session** command.

Example

Send a KUR to the CMPv2 server.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] quit
[Huawei] pki cmp keyupdate-request session test
 Info: Initializing configuration.
 Info: Creatting key update request packet.
 Info: Connectting to CMPv2 server.
 Error: CMPv2 server connect failed.
 Info: CMPv2 operation finish.
```

Related Topics

19.17.73 pki cmp session

19.17.73 pki cmp session

Function

The **pki cmp session** command creates a CMP session and displays the CMP session view, or displays the view of an existing CMP session.

The **undo pki cmp session** command deletes a CMP session.

By default, no CMP session exists.

Format

pki cmp session *session-name*

undo pki cmp session *session-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	It is a string of 1 to 63 case-insensitive characters without spaces or question marks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before choosing CMPv2 for certificate application, run the **pki cmp session** command to create a CMP session. CMPv2 configurations are performed in the CMP session view.

Example

Create the CMP session **test** and display the CMP session view.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test]
```

19.17.74 pki create-certificate

Function

The **pki create-certificate** command creates a self-signed certificate or local certificate.

Format

pki create-certificate [**self-signed**] **filename** *file-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
self-signed	Creates a self-signed certificate. If this parameter is not specified, a local certificate is created. • A self-signed certificate is issued by a PKI device itself. In a self-signed certificate, the certificate issuer and subject are the same. • A local certificate is issued by a PKI entity itself based on the certificate issued by CA. The issuer in a local certificate is CA.	-
filename *filename*	Specifies the name of a certificate file.	The value is a string of 1 to 64 case-insensitive characters without spaces or question marks.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a self-signed certificate or local certificate is generated by the device, the certificate file is saved in the storage device as a PEM file. You can export the certificate for other devices to use. This simplifies certificate issue process.

When you run the **pki create-certificate** command, the system asks you to enter certificate information, for example, PKI entity parameters, certificate file name, the validity time of certificate and RSA key length.

Precautions

The device does not provide lifecycle management for self-signed certificates. For example, self-signed certificates cannot be updated or revoked on the device. To ensure security of the device and certificates, a local certificate is recommended.

Example

Create a self-signed certificate **huawei**.

```
<Huawei> system-view
[Huawei] pki create-certificate self-signed filename huawei
```

 Copyright © Huawei Technologies Co., Ltd.

19.17.75 pki delete-certificate

Function

The **pki delete-certificate** command deletes a certificate from the memory.

Format

pki delete-certificate { **ca** | **local** | **ocsp** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ca	Deletes a CA certificate.	-
local	Deletes a local certificate.	-
ocsp	Deletes an Online Certificate Status Protocol (OCSP) server's certificate.	-
realm *realm-name*	Specifies the name of the PKI realm to which a certificate belongs.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the certificate expires or you want to apply for a new certificate, run this command to delete the CA, local, or OCSP server certificate from the memory.

Prerequisites

Example

Delete the local certificate from the memory.

```
<Huawei> system-view
[Huawei] pki delete-certificate local realm abc
```

Related Topics

19.17.103 pki realm (system view)

19.17.76 pki delete-certificate built-in-ca

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pki delete-certificate built-in-ca** command deletes an SSL decryption certificate from the memory.

Format

pki delete-certificate built-in-ca filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of the SSL decryption certificate file.	The SSL decryption certificate file name must already exist in the memory.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SSL decryption certificate expires or you want to apply for a new certificate, run the **pki delete-certificate built-in-ca** command to delete the current SSL decryption certificate from the memory. This command will not delete the certificate files in the device storage.

Prerequisites

The SSL decryption certificate has been imported to the memory using the **19.17.91 pki import-certificate built-in-ca** command.

Example

Delete an SSL decryption certificate from the memory.

```
<Huawei> system-view [Huawei] pki import-certificate built-in-ca filename test_builtinca.cer  Info: Succeeded in importing the built-in CA certificate.  [Huawei] pki delete-certificate built-in-ca filename test_builtinca.cer
```

Related Topics

19.17.91 pki import-certificate built-in-ca

19.17.77 pki delete-crl

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pki delete-crl** command deletes a CRL from the memory.

Format

pki delete-crl realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of the PKI realm that the certificate belongs to.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a CRL expires, run this command to delete a CRL file from the memory. This command will not delete the CRL files in storage card.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Example

Delete the CRL of PKI realm **abc** from the memory.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki delete-crl realm abc
```

Related Topics

19.17.103 pki realm (system view)

19.17.34 display pki crl

19.17.78 pki enroll-certificate

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pki enroll-certificate** command configures manual certificate enrollment.

Format

pki enroll-certificate realm *realm-name* [**pkcs10** [**filename** *filename*]] [**password** *password*]

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of a PKI realm.	The PKI realm name must already exist.
pkcs10	Uses the PKCS#10 format to display the local certificate request information. It can be used to request certificates in offline mode.	-
filename *filename*	Saves the certificate request information in a specified file. The certificate request information is saved in the file in PKCS#10 format and is sent to the CA in outband mode.	The value is a string of 1 to 64.
password *password*	Indicates a challenge password, which is used to request certificates in online mode. When the CA server processes the certificate request using the challenge password, you must set a challenge password on the entity, and the challenge password must be the same as the password configured on the CA server.	The value is a string of case-sensitive characters without question marks (?) or spaces. It can be a plain-text string of 1 to 64 characters or a cipher-text string of 48 to 108 characters. **NOTE** To improve certificate security, it is recommended that a password consist of at least two of the following: lowercase letters, uppercase letters, numerals and special characters. In addition, the password must contain at least 6 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Manual certificate application is online or offline.

- Online mode (in-band mode)

  In online requests, entities request certificates from CAs using the SCEP protocol. Then the entities store the obtained certificates on the sd1 of devices.
- Offline mode (out-of-band mode)

  The device generates a certificate request file. The administrator sends the file to the CA server using methods such as disks and emails.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Precautions

- If **pkcs10** is specified, an entity applies to a CA for a certificate in offline mode. The entity saves the certificate request information in a file in PKCS#10 format and sends the file to the CA in outband mode.
- If **pkcs10** is not specified, an entity applies to a CA for a certificate in online mode.
- In online mode, a PKI entity obtains a CA certificate and imports it to memory, and then obtains a local certificate and imports it to memory.
- After the **enrollment self-signed** command is used in the PKI realm, it is not allowed to use the **pki enroll-certificate** command to configure manual certificate enrollment.

Example

Enroll a certificate for the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki enroll-certificate realm abc
```

Related Topics

19.17.103 pki realm (system view)

19.17.79 pki entity

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pki entity** command creates a PKI entity and displays the PKI entity view, or displays the view of an existing PKI entity.

The **undo pki entity** command deletes a PKI entity.

By default, no PKI entity is configured.

Format

pki entity *entity-name*

undo pki entity *entity-name*

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A PKI entity refers to the applicant or user of a certificate. A PKI entity is required when you use PKI features. After a PKI entity is created, you can configure attributes for it, for example, common name, country code, email address, FQDN, IP address, geographic area, organization, department, state, and province. These attributes include identity information of the PKI entity. The identity information will be added to the subject of a PKI entity.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

Example

Configure a PKI entity **entity1** and enter the PKI entity view.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1]
```

 Copyright © Huawei Technologies Co., Ltd.

19.17.80 pki export-certificate

Function

The **pki export-certificate** command exports a certificate to the device storage.

Format

pki export-certificate { **ca** | **local** | **ocsp** } **realm** *realm-name* { **der** | **pem** | **pkcs12** }

Parameters

Parameter	Description	Value
ca	Exports a CA certificate.	-
local	Exports a local certificate.	-
ocsp	Exports the Online Certificate Status Protocol (OCSP) certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate.	The PKI realm name must already exist.
der	Exports a certificate in DER format.	-
pem	Exports a certificate in PEM format.	-
pkcs12	Exports a certificate in P12 format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To copy a certificate to another device, run the **pki export-certificate** command to export a certificate to the sd1 of the local device first, and then transfer the certificate to another device using a file transfer protocol.

Before using this command, run the **19.17.28 display pki certificate** command to view information about certificates on the device.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When the exported certificate file does not contain a private key, the device does not encrypt this file.

When you export the private key, the system asks you to enter the private key file name. If the private key file name and the certificate file name are the same, the private key and certificate are stored in the same file. If they are different, they are stored in different files.

When you export the private key, the system asks you to enter the private key file format and set the password. The password will be used when you run the **19.17.90 pki import-certificate** command to import this private key.

After the **enrollment self-signed** command is used in the PKI realm, you cannot use the **pki export-certificate** command to export certificates to files.

Example

Export the local certificate in the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki export-certificate local realm abc pem
 Please enter the name of certificate file <length 1-127>: aa
 If you only export the certificate, do not export the private key.
 You can directly enter empty of private key file.
 Please enter the name of private key file <length 1-127>:
 Info: Succeeded in exporting the certificate.
```

Related Topics

19.17.103 pki realm (system view)

19.17.90 pki import-certificate

19.17.28 display pki certificate

19.17.81 pki export-certificate default

Function

The **pki export-certificate default** command exports a default built-in certificate to the sd1.

Format

pki export-certificate default { **ca** | **local** } **filename** *filename*

Parameters

Parameter	Description	Value
ca	Specifies the CA certificate to be exported.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
local	Specifies the local certificate to be exported.	-
filename *filename*	Specifies the name of an exported certificate file.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.

Views

System view

Default Level

3: Management level

Usage Guidelines

To copy a certificate to another device, run this command to export the certificate to the sd1 on the local device first, and transfer the certificate file to the other device using a protocol transfer protocol.

Before using this command, run the **19.17.28 display pki certificate** command to view information about default built-in certificates on the device.

Example

Export the default built-in CA certificate.

```
<Huawei> system-view
[Huawei] pki export-certificate default ca filename ca.der
 Info: Succeeded in exporting the certificate.
```

Related Topics

19.17.28 display pki certificate

19.17.82 pki export built-in-ca rsa-key-pair

Function

The **pki export built-in-ca rsa-key-pair** command exports the RSA key pair to the sd1.

 Copyright © Huawei Technologies Co., Ltd.

Format

pki export built-in-ca rsa-key-pair *key-name* [**and-certificate** *certname*] { **pem** *file-name* [**3des** | **aes** | **des**] | **pkcs12** *file-name* } **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the RSA key pair name.	The value must be an existing RSA key pair name.
and-certificate *certname*	Indicates that the SSL decryption certificate is exported together with the associated RSA key pair.	The value must be an existing SSL decryption certificate name.
pem *file-name*	Indicates that the RSA key pair to be exported is in the PEM format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
pkcs12 *file-name*	Indicates that the RSA key pair to be exported is in the PKCS12 format and specifies the file name to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
3des | **aes** | **des**	Sets the encryption algorithm to AES, DES or 3DES if a file is exported in the PEM format. By default, AES is used. **NOTE** For security, DES and 3DES algorithms are not recommended.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password *password*	Specifies the password for the RSA key pair file. This password is used when you import an RSA key pair file.	The value is a string of 6 to 32 case-sensitive characters without question marks (?). To enhance security, a password must meet the minimum strength requirements, that is, the password needs to contain at least three types of the following characters: uppercase letters, lowercase letters, numerals, and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to transfer or back up the RSA key pair. After the configuration is complete, you can generate a PEM or PKCS12 file containing the RSA key pair (or also the SSL decryption certificate) in the flash.

Before using this command, run the **19.17.41 display pki rsa built-in-ca public** command to view information about the RSA key pair of the SSL decryption certificate.

Prerequisites

The RSA key pair has been created for the SSL decryption certificate using the **19.17.105 pki rsa built-in-ca** command with the **exportable** parameter specified, or the RSA key pair of the SSL decryption certificate has been imported to the memory using the **19.17.94 pki import built-in-ca rsa-key-pair** command with the **exportable** parameter specified.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

An RSA key pair is sensitive information. Delete or destroy the exported RSA key pair from your device or storage device immediately after you do not use it.

Example

Export RSA key pair **key2** to file **aaa.pem** and set the encryption method to AES.

```
<Huawei> system-view [Huawei] pki rsa built-in-ca key2 create exportable  Info: The name of the new key-pair will be: key2  The size of the public key ranges from 512 to 4096.  Input the bits in the modules:2048  Generating key-pairs... .......+++  ..............................+++  [Huawei] pki export built-in-ca rsa-key-pair key2 pem aaa.pem aes password Hello@123  Warning: Exporting the key pair impose security risks, are you sure you want to  export it? [y/n]:y                                                    Info: Succeeded in exporting the RSA key pair in PEM format.
```

Related Topics

19.17.94 pki import built-in-ca rsa-key-pair

19.17.91 pki import-certificate built-in-ca

19.17.41 display pki rsa built-in-ca public

19.17.83 pki export rsa-key-pair

Function

The **pki export rsa-key-pair** command exports the RSA key pair to the sd1 and allows the export of the associated certificate.

Format

pki export rsa-key-pair *key-name* [**and-certificate** *certificate-name*] { **pem** *file-name* [**3des** | **aes** | **des**] | **pkcs12** *file-name* } **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value must be an existing RSA key pair name.
and-certificate *certificate-name*	Indicates that the certificate related to the RSA key pair are exported.	The value must be an existing certificate file name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pem *file-name*	Indicates that the RSA key pair to be exported is in the PEM format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
pkcs12 *file-name*	Indicates that the RSA key pair to be exported is in the PKCS12 format and specifies the file name to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
3des | **aes** | **des**	Sets the encryption algorithm to DES, 3DES or AES if a file is exported in the PEM format. The default value is AES. **NOTE** DES and 3DES are less secure than AES and are not recommended.	-
password *password*	Specifies the encryption password for the RSA key pair file. This password is used when you import an RSA key pair file.	The value is a string of 6 to 32 case-sensitive characters without question marks (?). To enhance security, a password must contain at least two types of the following characters: uppercase letters, lowercase letters, numerals, and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%).

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To transfer or back up an RSA key pair, run this command to generate the PEM or PKCS12 file carrying this RSA key pair (which may include the certificate) in the sd1.

Before using this command, run the **19.17.42 display pki rsa local-key-pair** command to view information about the RSA key pairs on the device.

Prerequisites

The RSA key pair has been created and configured to be exportable using the **19.17.106 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **19.17.95 pki import rsa-key-pair** command.

Precautions

The RSA key pair is sensitive information. Delete and destroy the exported RSA key pair on the device or storage device immediately after you do not need it.

Example

Export the RSA key pair **key1** to the file **aaa.pem** and set the encryption method to AES.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create key1 exportable
 Info: The name of the new key-pair will be: key1
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
......+++
.....................+++
[Huawei] pki export rsa-key-pair key1 pem aaa.pem aes password Admin@1234
 Warning: Exporting the key pair impose security risks, are you sure you want to
 export it? [y/n]:y
 Info: Succeeded in exporting the RSA key pair in PEM format.
```

Related Topics

19.17.106 pki rsa local-key-pair create

19.17.95 pki import rsa-key-pair

19.17.42 display pki rsa local-key-pair

19.17.84 pki export sm2-key-pair

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pki export sm2-key-pair** command exports the SM2 key pair to the device storage.

Format

pki export sm2-key-pair *key-name* **der** *file-name*

pki export sm2-key-pair *key-name* **pem** *file-name* [**password** *password*]

Parameters

Parameter	Description	Value
key-name	Specifies the SM2 key pair name.	The value must be an existing SM2 key pair name.
der *file-name*	Exports the SM2 key pair as a DER file and specifies the file name.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
pem *file-name*	Exports the SM2 key pair as a PEM file and specifies the file name.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
password *password*	Specifies the password for the SM2 key pair file. This password is used when you import an SM2 key pair file.	The value is a string of 6 to 32 case-sensitive characters without question marks (?). For security purposes, the password must contain at least three types of the following: uppercase letters, lowercase letters, numerals, and special characters (such as ! @ # $ %).

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To transfer or back up an SM2 key pair, run this command to generate a file carrying this SM2 key pair in the device storage.

Before using this command, run the **19.17.43 display pki sm2 local-key-pair public (System view)** command to view information about the SM2 key pairs on the device.

Prerequisites

The RSA key pair has been created using the **19.17.109 pki sm2 local-key-pair create** command with the **exportable** parameter specified or the RSA key pair has been imported to the memory using the **19.17.96 pki import sm2-key-pair** command with the **exportable** parameter specified.

Precautions

An SM2 key pair is sensitive information. Delete or destroy the exported SM2 key pair from your device or storage device immediately after you do not use it.

Example

Export the SM2 key pair **key-1** to the file **aaa.pem**.

```
<Huawei> system-view
[Huawei] pki sm2 local-key-pair create key-1 exportable
 Info: The name of the new key-pair will be: key-1
 Generating key-pairs...
[Huawei] pki export sm2-key-pair key-1 pem aaa.pem password Admin@1234
 Warning: Exporting the key pair impose security risks, are you sure you want to
 export it? [y/n]:y
 Info: Succeeded in exporting SM2 key pair in PEM format.
```

Related Topics

19.17.109 pki sm2 local-key-pair create

19.17.96 pki import sm2-key-pair

19.17.43 display pki sm2 local-key-pair public (System view)

19.17.85 pki file-format

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pki file-format** command sets the format for the saved certificate request, certificate, and CRL.

By default, the device stores certificate request, certificate, and CRL in PEM format.

Format

pki file-format { **der** | **pem** }

Parameters

Parameter	Description	Value
der	Indicates that the format of a certificate request file is DER.	-
pem	Indicates that the format of a certificate request file is PEM.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To change the format for the saved certificate request, certificate, and CRL, for example, to use the certificate and CRL obtained through CMPv2, SCEP, or LDAP, run the **pki file-format** command.

However, the certificate and CRL obtained through HTTP are downloaded directly and are not saved in the format configured using this command. The created self-signed certificate or local certificate can only be saved in PEM format.

Example

Set the format of saved certificate request, certificate, and CRL to DER.

```
<Huawei> system-view
[Huawei] pki file-format der
```

19.17.86 pki generate built-in-ca certificate

Function

The **pki generate built-in-ca certificate** command generates an SSL decryption certificate.

Format

pki generate built-in-ca certificate rsa-key-pair *rsa-key-pair-name* **entity** *entity-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rsa-key-pair *rsa-key-pair-name*	Specifies the name of the RSA key pair in an SSL decryption certificate.	The RSA key pair must exist in the memory.
entity *entity-name*	Specifies the PKI entity name.	The PKI entity must have been configured and have a common name. If the PKI entity does not have a common name, an SSL decryption certificate cannot be generated.

Views

System view:

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable a proxy for SSL connection, the device complies with the certificate information on the real server and issues another certificate to the client using the SSL decryption certificate.

The generated SSL decryption certificate files are saved to the "sd1:/" directory.

Prerequisites

1. An RSA key pair of the SSL decryption certificate has been created using the **19.17.105 pki rsa built-in-ca** command or the RSA key pair has been imported to the memory of the device using the **19.17.94 pki import built-in-ca rsa-key-pair** command.
2. A PKI entity has been created using the **19.17.79 pki entity** command.
3. The common name of the PKI entity has been configured using the **19.17.17 common-name** command.

Example

Generate an SSL decryption certificate.

```
<Huawei> system-view
[Huawei] pki rsa built-in-ca rsakey create
 Info: The name of the new key-pair will be: rsakey
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....++++++
.....++++++
[Huawei] pki entity entity1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-pki-entity-entity1] common-name huawei
[Huawei-pki-entity-entity1] quit
[Huawei] pki generate built-in-ca certificate rsa-key-pair rsakey entity entity1
 Please enter the file name for built in CA certificate <length 1-64> : key1
Info: Generate built in CA certificate successfully.
```

Related Topics

19.17.105 pki rsa built-in-ca

19.17.94 pki import built-in-ca rsa-key-pair

19.17.79 pki entity

19.17.17 common-name

19.17.29 display pki certificate built-in-ca

19.17.87 pki get-certificate

Function

The **pki get-certificate** command downloads a certificate to the device storage.

Format

pki get-certificate { **ca** | **local** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ca	Specifies a CA or RA certificate to be obtained.	-
local	Specifies a local certificate to be obtained.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be obtained.	The value must be an existing PKI realm name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the SCEP method is used, the PKI entity queries and obtains issued certificates on the CA server and stores the certificates to the local storage. The

 Copyright © Huawei Technologies Co., Ltd.

PKI entity can download their own certificates, CA certificates, or local certificates of other entities.

The purposes of obtaining a certificate are as follows:

- Stores certificates to the device storage to improve certificate query efficiency and reduce the times of querying the PKI certificate repository.
- Prepares for certificate authentication.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command.

Precautions

After obtaining a CA certificate, the device automatically imports the certificate to the device memory. After the device obtains a local certificate, you need to import it to the memory manually.

If the same certificate exists on the device, delete the existing one; otherwise, the certificate cannot be obtained.

Example

Obtain the CA certificate in the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki get-certificate ca realm abc
```

Related Topics

19.17.103 pki realm (system view)

19.17.88 pki get-crl

Function

The **pki get-crl** command updates CRL immediately.

Format

pki get-crl realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of the CRL.	The value must be an existing PKI realm name.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CRL status is checked periodically when it is updated automatically. If the CRL on the device is likely to expire, configure this command to update CRL immediately.

After this command is executed, the new CRL replaces the old CRL in the storage, and is automatically imported to the memory to replace the old one.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command.

Example

Configure the CRL immediate update.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] quit
[Huawei] pki get-crl realm test
```

Related Topics

19.17.103 pki realm (system view)

19.17.89 pki http

Function

The **pki http** command configures a device to use HTTP to download a CA certificate, local certificate, or CRL.

Format

pki http [**esc**] *url-address save-name*

Parameters

Parameter	Description	Value
esc	Specifies the entering of URLs in the ASCII code.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
url-address	Specifies the URL of a CA certificate, local certificate, or CRL.	The value is a string of 1 to 128 case-sensitive characters.
save-name	Specifies the name of a CA certificate, local certificate, or CRL saved on the sd1 of the device.	The value is a string of 1 to 64 case-insensitive characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Before you configure a device to use HTTP to download a CA certificate, local certificate, or CRL, ensure that the sd1 of the device has enough space to accommodate the CA certificate, local certificate, or CRL.

Keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code, and **3f** is the hexadecimal ASCII code for the question mark (?). Therefore, the entered URL must be in **\x3f** format. For example, the URL that an administrator needs to enter is **http://www.***.com\x3fpage1**, instead of **http://www.***.com?page1**. If the administrator wants to configure **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the administrator should add an escape character (\) to \x3f and enter **http://www.***.com\x3fpage1\\x3f.**

Example

Configure a device to use HTTP to download a local certificate.

```
<Huawei> system-view
[Huawei] pki http http://10.1.1.1/test.cer local.cer
```

Configure a device to use HTTP to download a local certificate.

```
<Huawei> system-view
[Huawei] pki http esc http://www.***.com\x3fpage1\\x3f local.cer
```

19.17.90 pki import-certificate

Function

The **pki import-certificate** command imports a certificate to the device memory.

Format

pki import-certificate { **ca** | **local** } **realm** *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*] [**replace**] [**no-check-validate**] [**no-check-hash-alg**]

 Copyright © Huawei Technologies Co., Ltd.

pki import-certificate { **ca** | **local** } **realm** *realm-name* **pkcs12 filename** *filename* [**replace**] [**no-check-validate**] [**no-check-hash-alg**] **password** *password*

pki import-certificate ocsp realm *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*]

pki import-certificate ocsp realm *realm-name* **pkcs12 filename** *filename* **password** *password*

pki import-certificate realm *realm-name* **pem terminal password** *password*

Parameters

Parameter	Description	Value
ca	Imports a CA certificate. For example, when the device works as an SSL proxy, import the SSL proxy CA certificate and use the private key in the certificate to sign the SSL client certificate again.	-
local	Imports a local certificate.	-
realm *realm-name*	Specifies the PKI realm name of the imported certificate.	The PKI realm name must already exist. **NOTE** The domain name cannot contain spaces. Otherwise, the certificate cannot be imported.
der	Imports a certificate in DER format.	-
pkcs12	Imports a certificate in PKCS12 format.	-
pem	Imports a certificate in PEM format.	-
filename *filename*	Specifies the name of the imported certificate.	The file name must already exist.
replace	Deletes the original certificate and RSA key pair and imports the new certificate when there are repeated certificates in the domain. **NOTE** If the RSA key pair of the original certificate is not referenced by other domains, the certificate and key pair are deleted. If the RSA key pair of the original certificate is referenced by other domains or a CMP session, only the original certificate is deleted but the key pair is not deleted.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-check-validate	Specifies whether the validity check is performed on the imported certificate.	-
no-check-hash-alg	Specifies whether a check is performed on the hash algorithm used for the signature of the imported certificate.	-
ocsp	Imports the Online Certificate Status Protocol (OCSP) server's certificate.	-
terminal	Specifies the terminal import mode.	-
password *password*	Specifies the decryption password of the certificate, and the password is the same as the password set by the **19.17.80 pki export-certificate** command.	The value must be the name of an existing decryption password of the certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a certificate is saved to the storage, run this command to import the certificate to the memory for it to take effect.

The device supports the following certificate import modes:

- terminal: Import or copy the certificate file of the peer to the local device. That is, you can open the PEM certificate file using a text tool and copy the certificate content to the local device.
- file: The **filename** parameter is specified to import the certificate file of the peer.

Multiple certificates can be imported on the device, including the CA certificate, local certificate, and private key.

NOTE

If you do not know the format of the certificate you want to import, configure each format in turn and check whether the certificate is successfully imported.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The PKI realm has been created using the **19.17.103 pki realm (system view)** command, and the certificate file already exists on the storage device.

Precautions

If a certificate file contains a key pair file, the **pki import-certificate** command imports only the certificate file, but not the key pair file. To import the key pair file, run the **pki import rsa-key-pair** command after the **pki import-certificate** command, or run the **pki import rsa-key-pair** command to import the certificate and key pair files simultaneously.

It is not recommended that multiple local certificates be imported into the same PKI realm. Otherwise, certificate-related services may use the certificates that do not match the services, causing services to become unavailable.

When a certificate in **pkcs12** format is imported, the PKI system deletes the file name extension of the original certificate file, adds **_localx.cer** to generate a new file name, and saves it to the storage component. Therefore, the name of the certificate file to be imported should be less than 50 characters, so the total certificate file name does not exceed 64 characters, and the certificate file cannot be imported to the storage component.

When you import a certificate through a terminal, the key pair name is case-sensitive and contains 1 to 64 characters without spaces or question marks (?).

The device supports importing digital certificates generated through RSA encryption algorithms.

Example

Import a local certificate to PKI realm **abc** in file transfer mode.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki import-certificate local realm abc pem filename local.cer
 Info: Succeeded in importing the certificate.
```

Import a local certificate to the PKI realm **abc** in the terminal mode.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki import-certificate realm abc pem terminal password abc123
Enter encrypted private General Purpose key name:a
Please choise the key exportable: 1 (exportable):1
Enter PEM-formatted CA certificate.
End with a blank line or "end" on a line by itself.
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIQPLn9V3dmGr1LguLTIYI8RTANBgkqhkiG9w0BAQUFADBY
MRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGaHVhd2VpMRUw
EwYKCZImiZPyLGQBGRYFY2hpbmExEjAQBgNVBAMTCUNBIHNlcnZlcjAeFw0xMzEw
MTgwMjE4MzNaFw0xODEwMTgwMjI3NTlaMFgxEzARBgoJkiaJk/IsZAEZFgNjb20x
FjAUBgoJkiaJk/IsZAEZFgZodWF3ZWkxFTATBgoJkiaJk/IsZAEZFgVjaGluYTES
MBAGA1UEAxMJQ0Egc2VydmVyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEArdox+Z5U5T8D2W+dTihLydJ7+bMRF5Z1QDZvX8M9OmL01pTGKSq2LETqRDhT
u3N9L/yuYywylDeFXLsNL5KSYJVyV/VSUpawARiJ1EzWGke4Gdpqm+zQUpI5pxT
5SCwJKNcpQVPmPRpE1rmU/3czR/YzYHYkjO6sTqLDskOUBerjpMVx0J/y35EXSC/
7oiuXd/iU0W+unv97C4T7rZwpMtrn9RPpQtL95GacP8WlDCJjIopOQd//Q5POeAX
xLzfR87z8ri66UbrU8lU6/ZWlWma6hgIiBBfMLhgUdasDZ+neiNPEFdCZEdVEbm9
Of0X3GZU5XcoD7oNSa2s4diZFQIDAQABo4IBADCB/TATBgkrBgEEAYI3FAIEBh4E
AEMAQTALBgNVHQ8EBAMCAUYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUcLyj
kl6b2uhKC8Cq87bclb768yMwgZYGA1UdHwSBjjCBizCBiKCBhaCBgoY/aHR0cDov
L3owMDEzOTkwMWFiYy5jaGluYS5odWF3ZWkuY29tL0NlcnRFbnJvbGwvQ0ElMjBz
ZXJ2ZXIuY3Jshj9maWxlOi8vXFx6MDAxMzk5MDFhYmMuY2hpbmEuaHVhd2VpLmNv
```

 Copyright © Huawei Technologies Co., Ltd.

```
bVxDZXJ0RW5yb2xsXENBIHNlcnZlci5jcmwwEAYJKwYBBAGCNxUBBAMCAQAwDQYJ
KoZIhvcNAQEFBQADggEBAA2ROwrZ+0fQPs2FqdaoJp3QYA2pgJR8hGQ8n9vskVel
9UG3o7bsgmCPpfNb0k826Iuqur9PL7mQZvYmY+OH9tCC3zbwuJXrrZlfimFd9aH7
0V5MGRNuEkO5xPK2jNwHeg//Rnt7hCOnKiQP0/LBKRiEnXPrOoqtLgHaQsbu7gSs
HFHDoV+V1Hpo+n9Jtl0Eosi9g1gxCIueUOMT8eZC5coFHEIz661tXHcgwePK8lnh
Yfwc0YtJmbSr3gUVTztkrPODMf0msscVq8sZ3ewLfYqUlb85pt0c/GQwxSHYBfIe
JJopiEXZce1aMnwyScKjpyh8fbDOX3n6Uh/VeDCBnoU=
-----END CERTIFICATE-----
end
Enter PEM-formatted encrypted private General Purpose key.
End with "end" on a line by itself
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,F18D190B5CA99826

SFvJFyZUJbWlXOQh2cg4hh8yWW5fLeWw21rj9xn5P5ylsEtwxr+hZtgM+tGTW3BL
GzCgUkmnL+03EOaZXS4jW7v7lsNqciyvCPbeKGtSpPpGJ8MgVoqDdjAX1uKzPxsN
PcEbkMJd8Ak5o1PGv6fCtFmeFJVvTHGm/lyHtvn6aUy+riEywE4bgYNHc+C7NMHw
dIjICj31h4BAbTfBK4pyqxAL+nn3G5ayyAWlK/KYls3sEHHzScbyKQjuzIffkgNQ
ku/FcEvUvC69yBlp+75HEQG0WbpURfcCOBpLZrllxMpfrLVtMmE9HsrDeV6xG7XW
RbHeciBMjBN9zP0Pm0F0JdJp4I+Xv9CKWJ82KgigSHQTOKRVhgXp2Kryh7j4IVUh
tWOusOQC3/cKEDrhpx1sCHeRtXPA5/y3RZb6jGxx4iwkkK5qv/RN0W+4iNqZf6PO
KRKh6seR7h9F0eHQoTbT1uL5ow2SOSqfZOPnB9+t0qQBUSE4E8ZjsgohQBcTgQ8q
w21iiQZeyMHSrx6kiYsQxc1egxr8I/QV4OCEP9vH7tpu6vdnlc/WHBI7JhOV0u9Z
5sRm1ktOgfiqnpYVg+iB3wJtIVCtJiwvjSkLW0m+KdrrUiT9scPti7y0PReHacs/
fkjsey72T/mxPR24NJOpYYznF+whpwrCd3Io4lfxZDOzvUNtGD3ySbEcTe/PQBKj
TYcUlAn06VvCurYJV9jXqi9qt4tHKtQD0j7ToLTXpvTBYW0BaRULo1OZl9c+49B/
zlJfe3cU0VZpXOVowL5xPL6lvESDKjzQYRzKOBfJGwJs4OcBKGJ8XQ==
-----END RSA PRIVATE KEY-----
end
Enter PEM-formatted General Purpose certificate.
End with a blank line or "end" on a line by itself.
-----BEGIN CERTIFICATE-----
MIIFITCCBAmgAwIBAgIKGmoeqQAAAACZVDANBgkqhkiG9w0BAQUFADBYMRMwEQYK
CZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGaHVhd2VpMRUwEwYKCZIm
iZPyLGQBGRYFY2hpbmExEjAQBgNVBAMTCUNBIHNlcnZlcjAeFw0xNDAyMTAwNTU0
NTlaFw0xNTAyMTAwNjA0NTlaMAwxCjAIBgNVBAMTAWEwgZ8wDQYJKoZIhvcNAQEB
BQADgY0AMIGJAoGBAN5vT5A2Dy7iwTwNeisaWBecRi7SAzHyEer7U5ZzSsA/6xt9
LulqBoV8rMIsNe54flnxQww74QE8CBVkj1UJ5Fsq+S0UtU2fphSJkZMOVM0zmnPb
S6YyWoDOjR6JAKlxAgwYdAoO3iD/7xaIgtXrKQqj+dt7eieTSy5Z8dEWkJxAgMB
AAGjggK7MIICtzAdBgNVHQ4EFgQUOOMbU4dquenYHLpyaSP5cS3vNBgwHwYDVR0j
BBgwFoAUcLyjkl6b2uhKC8Cq87bclb768yMwggFJBgNVHR8EggFAMIIBPDCCATig
ggE0oIIBMIaBq2xkYXA6Ly8vQ049Q0ElMjBzZXJ2ZXIsQ049ejAwMTM5OTAxYWJj
LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxE
Qz1VbmF2YWlsYWJsZUNvbmZpZ0ROP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/
YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludIY/aHR0cDovL3ow
MDEzOTkwMWFiYy5jaGluYS5odWF3ZWkuY29tL0NlcnRFbnJvbGwvQ0ElMjBzZXJ2
ZXIuY3Jshj9maWxlOi8vXFx6MDAxMzk5MDFhYmMuY2hpbmEuaHVhd2VpLmNvbVxD
ZXJ0RW5yb2xsXENBIHNlcnZlci5jcmwwgeYGCCsGAQUFBwEBBIHZMIHWMGkGCCsG
AQUFBzAChl1odHRwOi8vejAwMTM5OTAxYWJjLmNoaW5hLmh1YXdlaS5jb20vQ2Vy
dEVucm9sbC96MDAxMzk5MDFhYmMuY2hpbmEuaHVhd2VpLmNvbV9DQSUyMHNlcnZl
ci5jcnQwaQYIKwYBBQUHMAKGXWZpbGU6Ly9cXHowMDEzOTkwMWFiYy5jaGluYS5o
dWF3ZWkuY29tXENlcnRFbnJvbGxcejAwMTM5OTAxYWJjLmNoaW5hLmh1YXdlaS5j
b21fQ0Egc2VydmVyLmNydDA/BgkrBgEEAYI3FAIEMh4wAEkAUABTAEUAQwBJAG4A
dABlAHIAbQBlAGQAaQBhAHQAZQBPAGYAZgBsAGkAbgBlMA0GCSqGSIb3DQEBBQUA
A4IBAQAQgqIzSVgOi1MOXIMNUREK35g/8zgPZwFw19jZeM5Jc0X7aJoV3PDFeCnA
pvzvKn/H/oB6UCSCX4RVdYhJI17ymSeBZUrq4XKsWOCPykwK34xc4cPpthQ9fcjc
pwHOq+JGWSfNsS9PBdzhxn+BrH4BlndMu3H/95bluf0kFNblyaZeuqwEmFkrJVxt
6u6PLVqhQyu0LhKUBMDavfi6e5/HEGaGoj18d2uUEYNWQOBcUoEhnnZ/7sCoTyRP
AsrXoUoS94lnX8z/GGK5nV+X6bvxbo6l0qyBtU/9Iax5MwLIXUBhzXUi0q5C5A2C
8KbFCoMv33ecr0ma94LRnn7qnVsr
-----END CERTIFICATE-----
end
 Successfully to import the certificate chain.
```

Related Topics

19.17.33 display pki credential-storage-path
19.17.103 pki realm (system view)

 Copyright © Huawei Technologies Co., Ltd.

19.17.80 pki export-certificate
19.17.89 pki http
19.17.97 pki ldap

19.17.91 pki import-certificate built-in-ca

Function

The **pki import-certificate built-in-ca** command imports the SSL decryption certificate to the memory.

Format

pki import-certificate built-in-ca filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the file name of the SSL decryption certificate.	The value must be the name of an existing SSL decryption certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Import the SSL decryption certificate to the memory to use it; otherwise, the certificate will not take effect.

When importing the SSL decryption certificate, make sure that the matching RSA key pair in the SSL decryption certificate exists on the device. The mapping relationship is created when the SSL decryption certificate is created. Search for the RSA key pair that corresponds to the SSL decryption certificate using the **19.17.69 pki built-in-ca match-rsa-key** command.

Prerequisites

The SSL decryption certificate file already exists on the storage device, and is generated using the **19.17.86 pki generate built-in-ca certificate** command.

Example

Import the SSL decryption certificate **key1_builtinca.cer** to the memory.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] pki generate built-in-ca certificate rsa-key-pair key1 entity entity1
 Please enter the file name for built in CA certificate <length 1-64> : key1_builtinca.cer
 Info: Generate built in CA certificate successfully.
[Huawei] pki import-certificate built-in-ca filename key1_builtinca.cer
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.86 pki generate built-in-ca certificate

19.17.69 pki built-in-ca match-rsa-key

19.17.92 pki import-certificate peer

Function

The **pki import-certificate peer** command imports a certificate of the remote device to the device memory.

Format

pki import-certificate peer *peer-name* { **der** | **pem** | **pkcs12** } **filename** [*filename*]

pki import-certificate peer *peer-name* **pkcs12 filename** *filename* **password** *password*

pki import-certificate peer *peer-name* **pem terminal**

Parameters

Parameter	Description	Value
peer-name	Specifies the name of peer certificate. A certificate cannot be imported to multiple peers.	The value is a string of 1 to 32 case-insensitive characters without spaces. If the character string is quoted by double quotation marks, it can contain spaces.
der	Imports a certificate of the remote device in DER format.	-
pem	Imports a certificate of the remote device in PEM format.	-
pkcs12	Imports a certificate of the remote device in P12 format.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
filename *filename*	Imports a certificate of the remote device in file mode.	The value is an existing name of certificate of the remote device.
password *password*	Specifies the decryption password of the certificate, and the password is the same as the password set by the **19.17.80 pki export-certificate** command.	The value must be the name of an existing decryption password of the certificate.
terminal	Imports a certificate of the remote device in terminal mode.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Where digital envelop authentication is used, configure the public key of the remote device. The public key can be obtained from the public and private key management module or certificate of the remote device.

The device supports the following certificate import modes:

- terminal: Import or copy the certificate file of the peer to the local device. That is, you can open the PEM certificate file using a text tool and copy the certificate content to the local device.
- file: The **filename** parameter is specified to import the certificate file of the peer.

Prerequisites

The certificate file of the remote device must already exist on the storage device.

Precautions

When a certificate in **pkcs12** format is imported, the PKI system deletes the file name extension of the original certificate file, adds **_localx.cer** to generate a new file name, and saves it to the storage component. Therefore, the name of the certificate file to be imported cannot exceed 50 characters. Otherwise, the total certificate file name will exceed 64 characters, and the certificate file cannot be imported to the storage component.

 Copyright © Huawei Technologies Co., Ltd.

You can import a peer certificate generated using the RSA encryption algorithm to the device.

Example

Import the certificate **aa.pem** of the remote device in the file mode.

```
<Huawei> system-view
[Huawei] pki import-certificate peer abcd pem file aa.pem
 Info: Succeeded in importing the peer certificate.
```

Import the certificate **aa.pem** of the remote device in the terminal mode.

```
<Huawei> system-view
[Huawei] pki import-certificate peer abcd pem terminal
Enter PEM-formatted peer certificate.
End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
MIIDvDCCAqSgAwIBAgIKEhk80wAAAAAEmjANBgkqhkiG9w0BAQUFADASMRAwDgYD
VQQDDAdDQV9ST09UMB4XDTEzMDIxOTEzMDAyMloXDTE0MDIxOTEzMTAyMlowDDEK
MAgGA1UEAxMBYTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC5i0dlqZntWLJjdGVW
0Qi7HY9O7XKiSu/YRT1T28jr31OeX8eWRmUUGqty6aJxyHrwUQzMObsUdX3xvIgs
py7pAgMBAAGjggHgMIIB3DAdBgNVHQ4EFgQU4luKA1gByOMUvBhb+b0AaFvRkE4w
HwYDVR0jBBgwFoAUzrrKOcetasuFF9CKjigCC1LU2SswQAYDVR0fBDkwNzA1oDOg
MYYvaHR0cDovLzEwLjEzNi41NS43Njo4MDgwL0NlcnRFbnJvbGwvQ0FfUk9PVC5j
cmwwggEVBggrBgEFBQcBAQSCAQcwggEDMIGjBggrBgEFBQcwAoaBlmxkYXA6Ly8v
Q049Q0FfUk9PVCxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1lc2FwLERDPWNvbT9jQUNlcnRp
ZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTBb
BggrBgEFBQcwAoZPaHR0cDovL2h1YXdlaS1uem01Z3cyZy5lc2FwLmNvbS9DZXJ0
RW5yb2xsL2h1YXdlaS1uem01Z3cyZy5lc2FwLmNvbV9DQV9ST09ULmNydDA/Bgkr
BgEEAYI3FAIEMh4wAEkAUABTAEUAQwBJAG4AdABlAHIAbQBlAGQAaQBhAHQAZQBP
AGYAZgBsAGkAbgBlMA0GCSqGSIb3DQEBBQUAA4IBAQC7i3evrt8uDL16KW52I619
aW0NFtkYgq1PUrPNHBr8NAAzNo1HKiAkUrcCdcyrO0z4KqmpT0b7wiEAwbXCZwyx
mSpie3FN58KTKbvssekogi93YewoZjXLXxUEc3fYJpF7olZ0UTML8QQoJLJxWK1c
+JYXDfe3X0u57Ql5vFQhxZuQ93shqlqqb1Hkec64NYsZkFGU5sJh+CRGhUypab2K
78JkuBmrC2vsNEGNQ0NE0RtMSiPNQFJ6LoxdtmJVk0XIPt6xUYLQu3y4CXuXCHuT
F0Coby3t9D42ECog40fh+63+l3OnU9D4Usq2Dujx32x6Nzm7gvkDyUpxZd9vN+a3
-----END CERTIFICATE-----

 Info: Succeeded in importing the peer certificate.
```

Related Topics

19.17.33 display pki credential-storage-path
19.17.39 display pki peer-certificate

19.17.93 pki import-crl

Function

The **pki import-crl** command imports the CRL to the memory.

Format

pki import-crl realm *realm-name* **filename** *file-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name.	The value must be an existing PKI realm name.
filename *file-name*	Specifies the name of an imported certificate or CRL file. The certificates only support the PEM and DER formats.	The value must be an existing certificate or CRL file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable the CRL that is obtained in out-of-band mode or is updated manually, run this command to import the CRL to the memory.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command and the CRL file has been downloaded using HTTP or LDAP.

Example

Import the CRL in the PKI realm to the memory.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki http esc http://www.***.com\x3fpage1\\x3f abc.crl
[Huawei] pki import-crl realm abc filename abc.crl
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.103 pki realm (system view)

19.17.89 pki http

19.17.97 pki ldap

19.17.34 display pki crl

 Copyright © Huawei Technologies Co., Ltd.

19.17.94 pki import built-in-ca rsa-key-pair

Function

The **pki import built-in-ca rsa-key-pair** command imports an RSA key pair in the SSL decryption certificate to the device memory.

Format

pki import built-in-ca rsa-key-pair *key-name* { **pem** | **pkcs12** } *file-name* [**exportable**] **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value is a string of 1 to 64 characters and case-sensitive without spaces or question marks (?). If the character string is quoted by double quotation marks (" "), the character string can contain spaces.
pem *file-name*	Specifies the format of the imported RSA key pair as PEM, and specifies the name of the RSA key pair file.	The value must be an existing certificate file name.
pkcs12 *file-name*	Specifies the format of the imported RSA key pair as PKCS12, and specifies the name of the RSA key pair file.	The value must be an existing certificate file name.
exportable	Specifies the imported RSA key pair as exportable.	-
password *password*	Specifies the decryption password of the RSA key pair, and the password is the same as the password set by the **19.17.82 pki export built-in-ca rsa-key-pair** command.	The value must be the name of an existing decryption password of the RSA key pair.

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When using the DSA key pair generated by other entities, store the RSA key pair on the sd1 of the local device. To make the RSA key pair take effect, run this command to import it to the memory.

Prerequisites

The RSA key pair must already exist on the storage device.

Example

Import RSA key pair **aaa.pem**. In the system, the RSA key pair name is **key-1** and password **Test!123**, and can be marked **exportable**.

```
<Huawei> system-view
[Huawei] pki import built-in-ca rsa-key-pair key-1 pem aaa.pem exportable password Test!123
 Info: Succeeded in importing the RSA key pair in PEM format.
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.82 pki export built-in-ca rsa-key-pair

19.17.95 pki import rsa-key-pair

Function

The **pki import rsa-key-pair** command imports the RSA key pair to the device memory.

Format

pki import rsa-key-pair *key-name* { **pem** | **pkcs12** } *file-name* [**exportable**] [**password** *password*]

pki import rsa-key-pair *key-name* **der** *file-name* [**exportable**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value is a string of 1 to 64 characters and case-sensitive without spaces or question marks (?). If the character string is quoted by double quotation marks (" "), the character string can contain spaces.
pem *file-name*	Indicates that the RSA key pair to be imported is in the PEM format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
pkcs12 *file-name*	Indicates that the RSA key pair to be imported is in the PKCS12 format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
der *file-name*	Indicates that the RSA key pair to be imported is in the DER format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
exportable	Indicates that the imported RSA key pair can be exported.	-
password *password*	Specifies the decryption password of the RSA key pair. , and the password is the same as the password set by the **19.17.83 pki export rsa-key-pair** command	The value must be the name of an existing decryption password of the RSA key pair. **NOTE** If the RSA key pair file does not have a decryption password, you need to enter any character. Otherwise, the import will fail.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to use the RSA key pair generated by other entities. After the configuration, the imported RSA key pair can be referenced by the PKI module for operations such as signing.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

If you do not know the format of the key pair you want to import, configure each format in turn and check whether the key pair is successfully imported.

Prerequisites

The RSA key pair must already exist on the storage device.

Example

Import RSA key pair **aaa.pem**. In the system, the RSA key pair name is **key-1**, and the password is **Test!123456**. The RSA key pair name can be marked **exportable**.

```
<Huawei> system-view
[Huawei] pki import rsa-key-pair key-1 pem aaa.pem exportable password Test!123456
 Info: Succeeded in importing the RSA key pair in PEM format.
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.83 pki export rsa-key-pair

19.17.96 pki import sm2-key-pair

Function

The **pki import sm2-key-pair** command imports the SM2 key pair to the device memory.

Format

pki import sm2-key-pair *key-name* **der** *file-name* [**exportable**]

pki import sm2-key-pair *key-name* **pem** *file-name* [**exportable**] [**password** *password*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
key-name	Specifies the name of the SM2 key pair to be imported on the device.	The value is a string of 1 to 64 characters and case-sensitive without spaces or question marks (?). If the character string is quoted by double quotation marks (" "), the character string can contain spaces.
der *file-name*	Specifies the format of the imported SM2 key pair as DER, and specifies the name of the file that stores the SM2 key pair.	The value must be an existing SM2 key pair name.
pem *file-name*	Specifies the format of the SM2 key pair to be imported as PEM, and specifies the name of the file that stores the SM2 key pair.	The value must be an existing SM2 key pair name.
exportable	Specifies the imported SM2 key pair as exportable.	-
password *password*	Specifies the decryption password of the SM2 key pair. The decryption password is the same as the password set by the **19.17.84 pki export sm2-key-pair** command.	The value must be the existing decryption password of the SM2 key pair.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to use the SM2 key pairs generated by other entities.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The SM2 key pair must already exist on the storage device.

Example

Import the SM2 key pair "**aaa.pem**" in the PEM format. The SM2 key pair is named **key-1** in the system with the decryption password **Admin@1234**, and is marked exportable.

```
<Huawei> system-view
[Huawei] pki import sm2-key-pair key-1 pem aaa.pem exportable password Admin@1234
 Info: Succeeded in importing SM2 key pair in PEM format.
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.97 pki ldap

Function

The **pki ldap** command configures a device to use LDAP to download a CA certificate, local certificate, or CRL.

Format

pki ldap ip *ip-address* **port** *port* **version** *version* [**attribute** *attr-value*] [**authentication** *ldap-dn ldap-password*] *save-name* **dn** *dn-value*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an LDAP server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of an LDAP server.	The value is an integer that ranges from 1 to 65535. The default value is 389.
version *version*	Specifies the version number of LDAP.	The value is an integer that ranges from 2 to 3. The default value is 3.
attribute *attr-value*	Specifies the attribute used by a device to request a certificate from an LDAP server.	The value is a string of 1 to 64 case-sensitive characters without question marks and spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
authentication *ldap-dn ldap-password*	Specifies the user name and password authenticated by the LDAP server.	*ldap-dn*: The value is a string of 1 to 64 case-sensitive characters without question marks and spaces. *ldap-password*: The value is a string of 1 to 32 case-sensitive characters without question marks and spaces.
save-name	Specifies the name of a CA certificate, local certificate, or CRL saved on the CF card or Hda1 of the device.	The value is a string of 1 to 64 case-insensitive characters without question marks and spaces.
dn *dn-value*	Specifies the DN used by a device to request a certificate from an LDAP server.	The value is a string of 1 to 128 case-sensitive characters, with spaces supported.

Views

System view

Default Level

3: Management level

Usage Guidelines

Note the following points when configuring a device to download a CA certificate, local certificate, or CRL through LDAP, the sd1 of the device has enough space for accommodating the CA certificate, local certificate, or CRL file to avoid downloading failed.

Example

Configure a device to download local certificate **local.cer** from the LDAP server with the IP address 10.1.1.1, port number 3389, and LDAP version number 2 and set the DN of the certificate to **admin**.

```
<Huawei> system-view
[Huawei] pki ldap ip 10.1.1.1 port 3389 version 2 local.cer dn admin
```

19.17.98 pki match-rsa-key

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pki match-rsa-key** command configures a device to search for the RSA key pair associated with a specific certificate.

Format

pki match-rsa-key certificate-filename *file-name*

Parameters

Parameter	Description	Value
certificate-filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Run this command to check the RSA key pair corresponding to a certificate. After configuration, the system searches for all the local RSA key pairs, compares them with the specified certificate and outputs the matched RSA key pair name once it is searched out.

Example

Configure a device to search for the RSA key pair that matches certificate file **local.cer**.

```
<Huawei> system-view
[Huawei] pki match-rsa-key certificate-filename local.cer
 Info: The file local.cer contains certificates 1.
 Info: Certificate 1 from file local.cer matches RSA key rsa2.key.
```

19.17.99 pki match-sm2-key

Function

The **pki match-sm2-key** command configures a device to search for the SM2 key pair associated with a specific certificate.

Format

pki match-sm2-key certificate-filename *file-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
certificate-filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Run this command to check the SM2 key pair corresponding to a certificate. After configuration, the system searches for all the local SM2 key pairs, compares them with the specified certificate and outputs the matched SM2 key pair name once it is searched out.

Example

Configure a device to search for the SM2 key pair that matches certificate file **sm2.cer**.

```
<Huawei> system-view
[Huawei] pki match-sm2-key certificate-filename sm2.cer
 Info: The file sm2.cer contains certificates 1.
 Info: Certificate 1 from file sm2.cer matches SM2 key sm2.key.
```

19.17.100 pki ocsp response cache enable

Function

The **pki ocsp response cache enable** command enables a device to cache OCSP responses.

The **undo pki ocsp response cache enable** command disables a device from caching OCSP responses.

By default, the PKI OCSP response cache function is disabled.

Format

pki ocsp response cache enable

undo pki ocsp response cache enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

After you enable a PKI entity to cache OCSP responses, the PKI entity first searches its cache for the certificate revocation status. If the search fails, the PKI entity sends a request to the OCSP server. In addition, the device caches valid OCSP responses for subsequent query. The OCSP responses have a validity period. With OCSP response cache enabled, a PKI entity refreshes the cached OCSP responses every minute to clear expired OCSP responses.

Example

Enable the PKI OCSP response cache function.

```
<Huawei> system-view
[Huawei] pki ocsp response cache enable
```

19.17.101 pki ocsp response cache number

Function

The **pki ocsp response cache number** command sets the maximum number of OCSP responses that can be cached on a PKI entity.

The **undo pki ocsp response cache number** command restores the maximum number of OCSP responses that can be cached on a PKI entity to the default value.

By default, the maximum number of OCSP responses that can be cached on a PKI entity is 2.

Format

pki ocsp response cache number *number*

undo pki ocsp response cache number

Parameters

Parameter	Description	Value
number	Specifies the maximum number of OCSP responses that can be cached on a PKI entity.	The value is an integer that ranges from 1 to 9.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

A PKI entity caches valid OCSP responses for subsequent query. If the number of cached OCSP responses reaches the value specified by *number*, the PKI entity stops caching OCSP responses.

Example

Set the maximum number of OCSP responses that can be cached on a PKI entity to 3.

```
<Huawei> system-view
[Huawei] pki ocsp response cache number 3
```

19.17.102 pki ocsp response cache refresh interval

Function

The **pki ocsp response cache refresh interval** command sets the interval at which the OCSP response cache is refreshed.

The **undo pki ocsp response cache refresh interval** command restores the interval at which a PKI entity refreshes the OCSP response cache to the default value.

By default, the interval at which a PKI entity refreshes the OCSP response cache is 5 minutes.

Format

pki ocsp response cache refresh interval *interval*

undo pki ocsp response cache refresh interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the OCSP response cache is refreshed.	The value is an integer that ranges from 1 to 1440, in minutes. The default value is 5.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

A PKI entity refreshes the OCSP response cache periodically and deletes the OCSP responses that have expired based on the *interval* value.

Example

Set the interval at which the OCSP response cache is refreshed to 30 minutes.

```
<Huawei> system-view
[Huawei] pki ocsp response cache refresh interval 30
```

19.17.103 pki realm (system view)

Function

The **pki realm** command creates a PKI realm and displays the PKI realm view, or displays the view of an existing PKI realm.

The **undo pki realm** command deletes a PKI realm.

By default, the device has a PKI realm named **default**. This realm can only be modified but cannot be deleted.

Format

pki realm *realm-name*

undo pki realm *realm-name*

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The value is a string of 1 to 63 case-insensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A PKI realm is a set of identity information required when a PKI entity enrolls a certificate.

Precautions

A PKI realm configured on a device is unavailable to certificate authorities (CAs) or other devices.

When a certificate is requested using a PKI realm, the system names the certificate file *PKI realm name*_**local.cer**. Therefore, if you will use a created PKI realm to request certificates, ensure that the PKI realm name length is shorter than 50 characters, because a certificate file with a name longer than 64 characters cannot be saved on a storage device.

Example

Create a PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc]
```

Related Topics

19.17.40 display pki realm

19.17.104 pki release-certificate peer

Function

The **pki release-certificate peer** command releases a certificate of the remote device.

Format

pki release-certificate peer { **name** *peer-name* | **all** }

Parameters

Parameter	Description	Value
name *peer-name*	Specifies the name of peer certificate to be released.	The value must be an existing peer certificate file name.
all	Releases all certificates of the remote device.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the specified certificate of the remote device is not required, run the **pki release-certificate peer** command to release the certificate of the remote device.

Before using this command, run the **19.17.39 display pki peer-certificate** command to view the certificate information of the remote device.

Prerequisites

The **19.17.92 pki import-certificate peer** command has been used to import the certificate of the remote device.

Example

Release the certificate **huawei** of the remote device.

```
<Huawei> system-view
[Huawei] pki release-certificate peer name huawei
 Info: Succeeded in releasing the peer certificate.
```

Related Topics

19.17.92 pki import-certificate peer

19.17.39 display pki peer-certificate

19.17.105 pki rsa built-in-ca

Function

The **pki rsa built-in-ca** command creates, overwrites, or destroys the RSA key pair in an SSL decryption certificate.

Format

pki rsa built-in-ca *key-name* { **create** [**exportable**] | **destroy** }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair in an SSL decryption certificate.	The value is a string of 1 to 64 case-sensitive characters without question marks and spaces. If the character string is quoted by double quotation marks, it can contain spaces and question marks.
create	Specifies the created RSA key pair of the SSL decryption certificate.	-
exportable	Specifies the created RSA key pair as exportable.	-
destroy	Specifies the destroyed RSA key pair of the SSL decryption certificate.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device uses the SSL decryption certificate to perform the proxy function for the SSL connection, the certificate must contain a public key. Run this command to create the RSA key pair of the SSL decryption certificate.

If the RSA key pair is referenced by the certificate and has been imported to the memory, you cannot overwrite or destroy the pair directly. To overwrite or destroy the RSA key pair, you can run the **19.17.76 pki delete-certificate built-in-ca** command to delete the SSL decryption certificate from the memory first.

When creating or overwriting the RSA key pair, you must enter the number of bits of the RSA key pair. The default value is 2048.

Precautions

The name of an RSA key pair cannot exceed 50 characters. Because when an RSA key pair is imported, if the certificate is imported at the same time, the PKI system adds **_builtinca.cer** after the name of the RSA key pair to generate a new certificate file name, and saves it to the storage component. If the name exceeds 50 characters, the total number of characters exceeds 64, and the certificate file cannot be saved to the storage component.

When creating the key pair, the system prompts the user to enter the number of bits of the RSA key pair. The longer the key pair, the harder it is to crack, and the

 Copyright © Huawei Technologies Co., Ltd.

more secure but slow the encryption algorithm. It is recommended that the number of bits of the RSA key pair exceed 2048; otherwise, it has security risks.

Example

Create an RSA key pair **rsakey**.

```
<Huawei> system-view
[Huawei] pki rsa built-in-ca rsakey create
 Info: The name of the new key-pair will be: rsakey
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....++++++
.....++++++
```

Related Topics

19.17.76 pki delete-certificate built-in-ca

19.17.41 display pki rsa built-in-ca public

19.17.106 pki rsa local-key-pair create

Function

The **pki rsa local-key-pair create** command creates the specified RSA key pair.

Format

pki rsa local-key-pair create *key-name* [**modulus** *modulus-size*] [**exportable**]

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair to be created.	The value is a string of 1 to 64 case-sensitive characters without question marks (?) and spaces. If the string is enclosed in double quotation marks (" "), the string can contain question marks (?) and spaces; however, if the string contains spaces, it cannot contain double quotation marks (").
modulus *modulus-size*	Specifies the size of the RSK key pair.	The value is an integer that ranges from: • AR100&AR120&AR150&AR160 &AR200 series: 2048 to 2048. The default value is 2048. • AR1200&AR2200&AR3200&AR3600 series: 2048 to 4096. The default value is 2048.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
exportable	Indicates that the new RSA key pair can be exported from the device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a PKI entity requests a certificate from the CA, the certificate enrollment request that it sends contains information such as the public key. Run this command to create the RSA key pair for the certificate request.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

Precautions

When creating the key pair, the system prompts the user to enter the number of bits of the RSA key pair. The longer the key pair, the harder it is to crack, and the more secure but slow the encryption algorithm. It is recommended that the number of bits of the RSA key pair exceed 2048; otherwise, it has security risks.

The name of an RSA key pair cannot exceed 50 characters. Because when an RSA key pair is imported, if the certificate is imported at the same time, the PKI system adds **_localx.cer** after the name of the RSA key pair to generate a new certificate file name, and saves it to the storage component. If the name exceeds 50 characters, the total number of characters exceeds 64, and the certificate file cannot be saved to the storage component.

The RSA key pair referenced by PKI realms cannot be overwritten. They can be overwritten only after the reference relationship is removed.

If the name of the new RSA key pair is the same as that of a pair on the device, the system prompts the user to decide whether to overwrite the existing pair.

Example

Create 2048-bit RSA key pair **test**.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create test
```

 Copyright © Huawei Technologies Co., Ltd.

```
Info: The name of the new key-pair will be: test
The size of the public key ranges from 2048 to 4096.
Input the bits in the modules:2048
Generating key-pairs...
......+++
.......+++
```

Related Topics

19.17.42 display pki rsa local-key-pair

19.17.107 pki rsa local-key-pair destroy

Function

The **pki rsa local-key-pair destroy** command deletes the specified RSA key pair.

Format

pki rsa local-key-pair destroy *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair to be deleted.	The value must be the name of an existing key pair.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

It is recommended that you run this command to destroy the specified RSA key pair if it is leaked, damaged, unused, or lost.

After this command is executed, the specified RSA key pair is deleted from the active device and the standby device.

Prerequisites

The RSA key pair has been created using the **19.17.106 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **19.17.95 pki import rsa-key-pair** command.

Precautions

The RSA key pair in the creation process cannot be deleted.

 Copyright © Huawei Technologies Co., Ltd.

The RSA key pair referenced by a PKI realm or CMP session cannot be deleted. They can be deleted only after the reference relationship is removed.

Example

Delete the RSA key pair **test**.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....+++
.....+++
[Huawei] pki rsa local-key-pair destroy test
 Warning: The name of the key pair to be deleted is test.
 Are you sure you want to delete the key pair? [y/n]:y
 Info: Delete RSA key pair success.
```

Related Topics

19.17.95 pki import rsa-key-pair

19.17.106 pki rsa local-key-pair create

19.17.108 pki set-certificate expire-prewarning

Function

The **pki set-certificate expire-prewarning** command sets the expiration warning date for the local certificate and the CA certificate in the memory.

The **undo pki set-certificate expire-prewarning** command restores the expiration warning date for the local certificate and the CA certificate in the memory to the default value.

By default, the expiration warning date for the local certificate and the CA certificate in the memory is seven days.

Format

pki set-certificate expire-prewarning *day*

undo pki set-certificate expire-prewarning

Parameters

Parameter	Description	Value
day	Specifies the expiration warning date.	The value is an integer that ranges from 7 to 180. By default, the value is 7.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

After this command is executed, you will be prompted the expiration of a certificate in advance. If the system detects that a certificate in the memory is to expire in less than *day*, the device sends an expiration warning to the user.

Example

Set the expiration warning date for the local certificate and the CA certificate in the memory as 30 days.

```
<Huawei> system-view
[Huawei] pki set-certificate expire-prewarning 30
```

19.17.109 pki sm2 local-key-pair create

Function

The **pki sm2 local-key-pair create** command creates an SM2 key pair.

Format

pki sm2 local-key-pair create *key-name* [**exportable**]

Parameters

Parameter	Description	Value
key-name	Specifies the name of the created SM2 key pair.	The value is a string of 1 to 64 case-sensitive characters without question marks (?) and spaces. If the string is enclosed in double quotation marks (" "), the string can contain question marks (?) and spaces; however, if the string contains spaces, it cannot contain double quotation marks (").
exportable	Specifies the created SM2 key pair as exportable.	-

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Run this command when the certificate needs to use the SM2 key pair.

Example

Create the SM2 key pair named abc.

```
<Huawei> system-view
[Huawei] pki sm2 local-key-pair create abc
 Info: The name of the new key-pair will be: abc
 Generating key-pairs...
```

Related Topics

19.17.43 display pki sm2 local-key-pair public (System view)

19.17.110 pki sm2 local-key-pair destroy

Function

The **pki sm2 local-key-pair destroy** command destroys an SM2 key pair.

Format

pki sm2 local-key-pair destroy *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the name of an SM2 key pair that you want to destroy.	The value must be an existing SM2 key pair name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

It is recommended that you run this command to destroy the specified SM2 key pair if it is leaked, damaged, unused or lost.

Prerequisites

The SM2 key pair has been created using the **19.17.109 pki sm2 local-key-pair create** command or the SM2 key pair has been imported to the memory using the **19.17.96 pki import sm2-key-pair** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Destroy the SM2 key pair named abc.

```
<Huawei> system-view
[Huawei] pki sm2 local-key-pair create abc
 Info: The name of the new key-pair will be: abc
 Generating key-pairs...
[Huawei] pki sm2 local-key-pair destroy abc
 Warning: The name of the key pair to be deleted is abc.
 Are you sure you want to delete the key pair? [y/n]:y
 Info: Succeeded in destroying SM2 key pair.
```

Related Topics

19.17.109 pki sm2 local-key-pair create
19.17.96 pki import sm2-key-pair

19.17.111 pki validate ocsp-server-certificate enable

Function

The **pki validate ocsp-server-certificate enable** command enables the function that uses the OCSP server certificate to verify OCSP server packets.

The **undo pki validate ocsp-server-certificate enable** command disables the function that uses the OCSP server certificate to verify OCSP server packets.

By default, the function that uses the OCSP server certificate to verify OCSP server packets is disabled.

Format

pki validate ocsp-server-certificate enable

undo pki validate ocsp-server-certificate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

For security purposes, you are advised to enable the function that uses the OCSP server certificate to verify OCSP server packets. If OCSP server packets fail the verification, the device discards these packets.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If the imported OCSP server certificate is not the correct one, OCSP server packets fail the verification, causing the local certificate to become unavailable. To prevent this problem, import the correct OCSP server certificate. If no OCSP server certificate can be obtained, run the **undo pki validate ocsp-server-certificate enable** command to disable the function that uses the OCSP server certificate to verify OCSP server packets.

Example

Enable the function that uses the OCSP server certificate to verify OCSP server packets.

```
<Huawei> system-view
[Huawei] pki validate ocsp-server-certificate enable
```

19.17.112 pki validate-certificate

Function

The **pki validate-certificate** command allows you to verify the validity of a CA certificate or a local certificate.

Format

pki validate-certificate { **ca** | **local** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ca	Checks validity of the CA certificate.	-
local	Checks validity of the local certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When an end entity verifies a peer certificate, it checks the status of the peer certificate. For example, the end entity checks whether the peer certificate has expired and whether the certificate is in a CRL.

To verify the validity of a CA certificate or a local certificate, run the **pki validate-certificate** command.

Prerequisites

A PKI realm has been configured using the **pki realm (system view)** command.

Precautions

The **pki validate-certificate ca** command allows you to verify only the root CA certificate, but not subordinate CA certificates. When multiple CA certificates are imported on a device, you can use only the **pki validate-certificate local** command to verify the validity of subordinate certificates.

Example

Configure the device to check validity of the local certificate using CRL.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] certificate-check crl
[Huawei-pki-realm-abc] quit
[Huawei] pki validate-certificate local realm abc
```

19.17.113 reset pki cmp statistics

Function

The **reset pki cmp statistics** command clears the statistics on CMP sessions.

Format

reset pki cmp statistics [**session** *session-name*]

Parameters

Parameter	Description	Value
session *session-name*	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

User view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If a CMP session is specified, the statistics of the session is cleared. If no CMP session is specified, the statistics of all sessions is cleared.

Example

Clear statistics on CMP session **test**.

```
<Huawei> reset pki cmp statistics session test
```

19.17.114 reset pki ocsp response cache

Function

The **reset pki ocsp response cache** command resets an OCSP response cache.

Format

reset pki ocsp response cache

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The PKI entity caches valid OCSP responses for future searches. If the number of cached OCSP responses reaches the maximum value, no more OCSP responses can be cached. To ensure that the latest OCSP responses can be cached, you can run this command to clear the OCSP response cache first.

Example

Reset an OCSP response cache.

```
<Huawei> reset pki ocsp response cache
```

19.17.115 reset pki ocsp server down-information

Function

The **reset pki ocsp server down-information** command clears the DOWN status information of the OCSP server recorded on the device.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset pki ocsp server down-information [**url** [**esc**] *url-addr*]

Parameters

Parameter	Description	Value
url [**esc**] *url-addr*	Specifies the OCSP server's URL address. If no URL address is specified, clear the DOWN status information on all OCSP servers. If the **esc** parameter is specified, the URL address in ASCII format is supported.	The value is a string starting with http:// and consisting of 1 to 128 case-sensitive characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

There is a mechanism to determine whether the OCSP server is down. When the OCSP server corresponding to a URL cannot be accessed, the server status is set to DOWN. In this case, the device will not send OCSP requests to the URL for 10 minutes.

However, this mechanism may falsely set the state of a transiently disconnected server to DOWN. Using this command, the user can manually clear the falsely reported DOWN state of the OCSP server so that the device can send OCSP requests to the server.

The keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

Clear the OCSP server DOWN information of the specified URL.

```
<Huawei> reset pki ocsp server down-information
```

 Copyright © Huawei Technologies Co., Ltd.

19.17.116 rsa local-key-pair

Function

The **rsa local-key-pair** command configures the RSA key pair used to request a certificate using the SCEP or in an offline mode.

The **undo rsa local-key-pair** command deletes the RSA key pair used to request a certificate using the SCEP or in an offline mode.

By default, the system does not configure the RSA key pair used to request a certificate using the SCEP or in an offline mode.

Format

rsa local-key-pair *key-name*

undo rsa local-key-pair

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair.	The value must be an existing RSA key pair name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The PKI entity that requests a certificate from the CA using the SCEP or in offline PKCS#10 mode must contain a public key. Run this command to configure the RSA key pair.

Prerequisites

The RSA key pair for certificate application has been created using the **19.17.106 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **19.17.95 pki import rsa-key-pair** command.

Precautions

An RSA key pair can be specified to only one PKI.

Example

Configure the RSA key pair that is referenced by the PKI realm **test**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....+++
.....
.....+++
[Huawei] pki realm test
[Huawei-pki-realm-test] rsa local-key-pair test
```

Related Topics

19.17.106 pki rsa local-key-pair create
19.17.95 pki import rsa-key-pair

19.17.117 serial-number

Function

The **serial-number** command adds the serial number of a device to the PKI entity.

The **undo serial-number** command restores the default setting.

By default, the serial number of a device is not added to the PKI entity.

Format

serial-number

undo serial-number

Parameters

None

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity include the identity information of the PKI entity. The CA identifies a certificate applicant based on identity information provided by a PKI entity. To further identify the applicant, add the serial number of the device to the PKI entity.

After the serial number of the device is added to a PKI entity, the certificate request packet sent by the device to the CA server carries this serial number. After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the device serial number.

 Copyright © Huawei Technologies Co., Ltd.

Example

Add the serial number of the device to a PKI entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] serial-number
```

Related Topics

19.17.35 display pki entity

19.17.118 sm2 local-key-pair

Function

The **sm2 local-key-pair** command configures the SM2 key pair used to request a certificate in an offline mode.

The **undo sm2 local-key-pair** command deletes the SM2 key pair used to request a certificate in an offline mode.

By default, the system does not configure the SM2 key pair used to request a certificate in an offline mode.

Format

sm2 local-key-pair *key-name*

undo rsa local-key-pair

Parameters

Parameter	Description	Value
key-name	Specifies the name of the SM2 key pair.	The value must be an existing SM2 key pair name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The PKI entity that requests a certificate from the CA in offline PKCS#10 mode must contain a public key. Run this command to configure the SM2 key pair.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The SM2 key pair for certificate application has been created using the **19.17.109 pki sm2 local-key-pair create** command or the SM2 key pair has been imported to the memory using the **19.17.96 pki import sm2-key-pair** command.

Precautions

An SM2 key pair can be specified to only one PKI.

Example

Configure the SM2 key pair that is referenced by the PKI realm **test**.

```
<Huawei> system-view
[Huawei] pki sm2 local-key-pair create test
 Info: The name of the new key-pair will be: test
 Generating key-pairs...
[Huawei] pki realm test
[Huawei-pki-realm-test] sm2 local-key-pair test
```

Related Topics

19.17.109 pki sm2 local-key-pair create

19.17.96 pki import sm2-key-pair

19.17.40 display pki realm

19.17.119 source interface

Function

The **source interface** command configures the source interface used in TCP connection setup.

The **undo source interface** command restores the default source interface used in TCP connection setup.

By default, the device uses the outbound interface as the source interface for TCP connection setup.

Format

source interface *interface-type interface-number*

undo source interface

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies an interface's IP address as the source IP address used in TCP connection setup. • *interface-type* indicates the type of the interface. • *interface-number* indicates the number of the interface.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **source interface** command specifies the source interface for establishing a connection between the device and the Simple Certificate Enrollment Protocol (SCEP) or Online Certificate Status Protocol (OCSP) server. This interface IP address is the source IP address of the TCP connection.

In the multi-output scenario, if the interfaces for sending and receiving a TCP packet are different, the IP address in the received TCP packet is different from the IP address of the receiving interface. Then the TCP packet is dropped, and the TCP connection is torn down. In this situation, you can run this command to specify the loopback interface address.

Precautions

Ensure that the interface is at Layer 3 and has an IP address configured.

Example

Configure the source interface used in TCP connection setup to Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip address 10.136.2.25 24
[Huawei-Ethernet2/0/0] quit
[Huawei] pki realm abc
[Huawei-pki-realm-abc] source interface ethernet 2/0/0
```

19.17.120 state (PKI entity view)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **state** command configures a state or province name for an entity.

The **undo state** command deletes the configuration.

By default, no state or province name is configured for a PKI entity.

Format

state *state-name*

undo state

Parameters

Parameter	Description	Value
state-name	Specifies the state or province name of an entity.	The value is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a state or province name for a PKI entity.

After the state or province name is configured for a PKI entity, the certificate request packet sent by the device to the CA server contains this province name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the state or provision name of the PKI entity.

Example

Configure the province name to **Jiangsu** for a PKI entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] state Jiangsu
```

Related Topics

19.17.35 display pki entity

 Copyright © Huawei Technologies Co., Ltd.

19.17.121 undo pki cmp poll-request session

Function

The **undo pki cmp poll-request session** command cancels CMP polling requests.

Format

undo pki cmp poll-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of the CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the server cannot deliver the results immediately after the client initiates certificate-related requests, the server requires the client to send the requests in polling mode until the server deliver the final result. The process duration varies with the actual situation. To cancel the process, run the command. In that, the certificate-related request is also canceled.

Prerequisites

A CMP session has been created using the **19.17.73 pki cmp session** command.

Example

Cancel CMP polling requests.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] quit
[Huawei] undo pki cmp poll-request session test
```

Related Topics

19.17.73 pki cmp session

 Copyright © Huawei Technologies Co., Ltd.

19.17.122 validate time disable

Function

The **validate time disable** command ignores time check in PKI certificate authentication.

The **undo validate time disable** command restores the default configuration.

By default, time is checked in PKI certificate authentication.

NOTE

Only AR100&AR120&AR150 series, AR161, AR161W, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S among the AR160 series support this command.

Format

validate time disable

undo validate time disable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device verifies the time during PKI certificate verification. If the time does not match, the PKI certificate verification fails. If the device does not support the clock synchronization function and restarts due to causes such as power-off, the system time is restored to the factory setting and an error occurs in PKI certificate verification. To avoid this problem, the administrator can run this command to disable the device from verifying the time during PKI certificate verification.

Precautions

After the **validate time disable** is run, the device will not generate certificate expiration logs.

Example

Ignore time check in PKI certificate authentication.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] PKI realm test
[Huawei-pki-realm-test] validate time disable
```

19.17.123 vpn-instance

Function

The **vpn-instance** command adds a PKI to a specified VPN.

The **undo vpn-instance** command unbinds a PKI from a specified VPN.

By default, a PKI does not belong to any VPN.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be the name of an existing VPN instance.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain and verify certificates, the device needs to communicate with the CA or SCEP server. When the CA or SECP server is in a VPN, add the PKI to the specified VPN.

Prerequisites

1. A VPN instance has been created using the **12.9.35 ip vpn-instance** command.
2. The RD has been configured using the **12.9.50 route-distinguisher** command.

Example

Add the PKI to the VPN named **vrf1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] route-distinguisher 22:1
[Huawei-vpn-instance-vrf1-af-ipv4] quit
[Huawei-vpn-instance-vrf1] quit
[Huawei] pki realm abc
[Huawei-pki-realm-abc] vpn-instance vrf1
```

Related Topics

12.9.35 ip vpn-instance

12.9.50 route-distinguisher

19.18 SSL Configuration Commands

19.18.1 ciphersuite

Function

The **ciphersuite** command configures cipher suites in a server SSL policy.

The **undo ciphersuite** command restores the default configuration.

By default, a server SSL policy supports the cipher suites: **ecdhe_rsa_aes128_gcm_sha256**, **ecdhe_rsa_aes256_gcm_sha384**, **rsa_aes_128_sha256**, and **rsa_aes_256_sha256**.

Format

ciphersuite { **rsa_3des_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_sha256** | **rsa_aes_256_sha256** | **rsa_aes128_ccm** | **rsa_aes128_gcm_sha256** | **rsa_aes256_ccm** | **rsa_aes256_gcm_sha384** | **ecdhe_rsa_aes128_gcm_sha256** | **ecdhe_rsa_aes256_gcm_sha384** } *

undo ciphersuite

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rsa_3des_cbc_sha	Indicates the **rsa_3des_cbc_sha** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 3DES_CBC algorithm to encrypt data, and the SHA algorithm to compute the MAC. **NOTE** RSA: Rivest-Shamir-Adleman DES: Data Encryption Standard CBC: Cipher Block Chaining SHA: Secure Hash Algorithm	-
rsa_aes_128_cbc_sha	Indicates the **rsa_aes_128_cbc_sha** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_CBC to encrypt data, and the SHA algorithm to compute the message authentication code (MAC). **NOTE** AES: Advanced Encryption Standard	-
rsa_aes_128_sha256	Indicates the **rsa_aes_128_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_CBC to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rsa_aes_256_sha256	Indicates the **rsa_aes_256_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 256-bit AES_CBC to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-
rsa_aes128_ccm	Indicates the **rsa_aes128_ccm** cipher suite. This cipher suite uses the RSA algorithm to compute the key and the 128-bit AES_CCM to encrypt data. **NOTE** CCM: Counter with CBC-MAC	-
rsa_aes128_gcm_sha256	Indicates the **rsa_aes128_gcm_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_GCM to encrypt data, and the SHA2-256 algorithm to compute the MAC. **NOTE** GCM: Galois/Counter Mode	-
rsa_aes256_ccm	Indicates the **rsa_aes256_ccm** cipher suite. This cipher suite uses the RSA algorithm to compute the key and the 256-bit AES_CCM to encrypt data.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rsa_aes256_gcm_sha384	Indicates the **rsa_aes256_gcm_sha384** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 256-bit AES_GCM to encrypt data, and the SHA2-384 algorithm to compute the MAC.	-
ecdhe_rsa_aes128_gcm_sha256	Indicates the **ecdhe_rsa_aes128_gcm_sha256** cipher suite. This cipher suite uses the ECDHE RSA algorithm to compute the key, the 128-bit AES_GCM to encrypt data, and the SHA2-256 algorithm to compute the MAC. **NOTE** GCM: Galois/Counter Mode ECDHE: Elliptic Curve Diffie-Hellman with Ephemeral keys	-
ecdhe_rsa_aes256_gcm_sha384	Indicates the **ecdhe_rsa_aes256_gcm_sha384** cipher suite. This cipher suite uses the ECDHE RSA algorithm to compute the key, the 256-bit AES_GCM to encrypt data, and the SHA2-384 algorithm to compute the MAC.	-

Views

Server SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

A cipher suite consists of a data encryption algorithm, a key exchange algorithm, and a MAC algorithm. During an SSL handshake, an SSL client sends a Client Hello message to notify an SSL server of the SSL protocol version and cipher suites that it supports. The SSL server determines the SSL protocol version and cipher suite used for this communication and sends a Server Hello message to notify the client.

The **ciphersuite** command configures the cipher suite that the Router can use when it functions as an SSL server.

Configuration Impact

To ensure high security, you are not advised to configure the cipher suite supported by the server SSL policy to **rsa_3des_cbc_sha** and **rsa_aes_128_cbc_sha**.

Using the **ecdhe_rsa_aes128_gcm_sha256** or **ecdhe_rsa_aes256_gcm_sha384** algorithm will affect the SSL server performance.

Example

Configure a server SSL policy to use the **rsa_aes_256_sha256** cipher suite.

```
<Huawei> system-view
[Huawei] ssl policy users type server
[Huawei-ssl-policy-users] ciphersuite rsa_aes_256_sha256
```

Related Topics

19.18.10 ssl policy

19.18.2 display ssl connection statistics

Function

The **display ssl connection statistics** command displays statistics on SSL connections.

Format

display ssl connection statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When a device sets up a connection with an SSL server or client, the device automatically counts and records the SSL connection.

This command displays the maximum number of SSL connections within a certain period so that the administrator can perform SSL fault diagnosis and troubleshooting quickly.

Example

View statistics on SSL connections.

```
<Huawei> display ssl connection statistics
------------------------------------------------------------------------------
Maximum of total connections in history          :   100
Begin time of total connections                  :   2013-09-26 12:19:11
Maximum time of total connections                :   2013-09-26 12:19:11
------------------------------------------------------------------------------
```

Table 19-175 Description of the display ssl connection statistics command output

Item	Description
Maximum of total connections in history	Maximum number of SSL connections in history.
Begin time of total connections	Time when the system starts to count SSL connections.
Maximum time of total connections	Time when the system records the maximum number of SSL connections.

Related Topics

19.18.7 reset ssl connection statistics

19.18.3 display ssl policy

Function

Using the **display ssl policy** command, you can view information about an SSL policy.

Format

display ssl policy [*policy-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy. If this parameter is not specified, the system displays information about all SSL policies.	The SSL policy name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about all SSL policies or a specified SSL policy.

Example

Display information about all SSL policies.

```
<Huawei> display ssl policy
Policy number: 2
  ------------------------------------------------------------------------------
  policy ID   policy name                policy type     bind number
  ------------------------------------------------------------------------------
  1           client-users               Client          0
  2           server-users               Server          0
  ------------------------------------------------------------------------------
```

Display information about the client SSL policy **client-users**.

```
<Huawei> display ssl policy client-users
  ------------------------------------------------------------------------------
  Policy name                        :   client-users
  Policy ID                          :   2
  Policy type                        :   Client
  Cipher suite                       :   rsa_aes128_sha256
                                         rsa_aes256_sha256
  PKI realm                          :   -
  Version                            :   tls1.2
  Server verify                      :   1
  CA certificate chain load status   :   unloaded
  CA certificate num                 :   0
  Local certificate load status      :   unloaded
  SSL renegotiation status           :   enable
  Bind number                        :   0
  SSL connection number              :   0
------------------------------------------------------------------------------
```

Display information about server SSL policy **server-users**.

```
<Huawei> display ssl policy server-users
  ------------------------------------------------------------------------------
  Policy name                        :   server-users
```

 Copyright © Huawei Technologies Co., Ltd.

```
Policy ID                       :  3
Policy type                     :  Server
Cipher suite                    :  rsa_aes128_sha256
                                rsa_aes256_sha256
PKI realm                       :  -
Version                         :  tls1.2
Cache number                    :  128
Time out(second)                :  3600
Local certificate load status   :  unloaded
CA certificate chain load status:  unloaded
SSL renegotiation status        :  enable
Bind number                     :  0
SSL connection number           :  0
------------------------------------------------------------------------------
```

Table 19-176 Description of the display ssl policy command output

Item	Description
Policy name	Name of an SSL policy. To configure an SSL policy, run the **ssl policy** command.
Policy ID	ID of an SSL policy.
Policy type	Type of an SSL policy: client SSL policy or server SSL policy. To configure an SSL policy, run the **ssl policy** command.
Cipher suite	Cipher suite used by the SSL policy. • To configure a client SSL policy, run the **19.18.5 prefer-ciphersuite** command. • To configure a server SSL policy, run the **19.18.1 ciphersuite** command.
PKI realm	PKI domain used by the SSL policy. To configure the PKI domain, run the **19.18.4 pki-realm** command.
Version	Version of the SSL protocol used by the client SSL policy. • ssl3.0 • tls1.0 • tls1.1 • tls1.12 To specify the SSL version, run the **19.18.12 version (Client SSL policy view)** command.
Server verify	Whether the SSL client is enabled to authenticate an SSL server. • 1: enabled • 0: disabled

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CA certificate chain load status	Whether the CA certificate chain has been loaded to the SSL client. • loaded: The certificate chain has been loaded to the SSL client. • unloaded: The certificate has not been loaded to the SSL client. • got but unloaded: The SSL client has obtained the certificate chain but has not loaded it.
CA certificate num	Number of CA certificates in the certificate chain.
Local certificate load status	Local certificate loading status. **loaded** indicates that the certificate has been loaded. **unloaded** indicates that the certificate is not loaded. **pending** indicates that the certificate is being generated.
SSL renegotiation status	SSL renegotiation status. • enable • disable
Bind number	Whether an SSL policy has been applied to an application layer protocol such as HTTP. • 1: yes • 0: no To apply an SSL policy to HTTP, run the **19.19.4 http secure-server ssl-policy** command.
SSL connection number	Number of SSL connections established by using an SSL policy.
Cache number	Maximum number of sessions that can be saved on the SSL server. To configure a session, run the **session** command.
Time out(second)	Timeout period of a saved session. To configure a session, run the **session** command.

19.18.4 pki-realm

Function

Using the **pki-realm** command, you can specify a public key infrastructure (PKI) domain in an SSL policy.

Using the **undo pki-realm** command, you can delete the PKI domain from the SSL policy.

By default, the PKI domain **default** exists on the device. This domain can be modified, but cannot be deleted.

 Copyright © Huawei Technologies Co., Ltd.

Format

pki-realm *realm-name*

undo pki-realm

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI domain.	The PKI domain name must already exist.

Views

Client SSL policy view, server SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command specifies a PKI domain in an SSL policy. A PKI domain has different functions when it is specified in a server SSL policy and a client SSL policy:

- After a PKI domain is specified in the server SSL policy view, the Router functioning as an SSL server obtains a digital certificate from the certificate authority (CA) specified in the PKI domain. Then SSL clients authenticate the Router by checking the digital certificate.
- After a PKI domain is specified in the client SSL policy view, the Router functioning as an SSL client obtains a CA certificate chain from the CA specified in the PKI domain. If SSL server authentication is enabled by using the **server-verify enable** command, the Router authenticates the SSL server using the CA certificate chain.

Prerequisites

A PKI domain has been created.

Precautions

When the SSL policy is referenced by another configuration, you cannot modify the configuration using the **pki-realm** command.

When functioning as an SSL server, the Router is authenticated by SSL clients, but it cannot authenticate SSL clients.

When functioning as an SSL client, the Router does not allow SSL servers to authenticate it, but it can authenticate SSL servers.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a client SSL policy to use the PKI domain **client-realm**.

```
<Huawei> system-view
[Huawei] ssl policy users type client
[Huawei-ssl-policy-users] pki-realm client-realm
```

Related Topics

19.18.10 ssl policy

19.18.8 server-verify enable

19.17.103 pki realm (system view)

19.18.5 prefer-ciphersuite

Function

The **prefer-ciphersuite** command configures cipher suites in a client SSL policy.

The **undo prefer-ciphersuite** command restores the default configuration.

By default, a client SSL policy uses the cipher suites: **ecdhe_rsa_aes128_gcm_sha256**, **ecdhe_rsa_aes256_gcm_sha384**, **rsa_aes_128_sha256**, and **rsa_aes_256_sha256**.

Format

prefer-ciphersuite { **rsa_3des_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_sha256** | **rsa_aes_256_sha256** | **rsa_aes128_ccm** | **rsa_aes128_gcm_sha256** | **rsa_aes256_ccm** | **rsa_aes256_gcm_sha384** | **ecdhe_rsa_aes128_gcm_sha256** | **ecdhe_rsa_aes256_gcm_sha384** } *

undo prefer-ciphersuite

Parameters

Parameter	Description	Value
rsa_3des_cbc_sha	Indicates the **rsa_3des_cbc_sha** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 3DES_CBC algorithm to encrypt data, and the SHA algorithm to compute the MAC.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rsa_aes_128_cbc_sha	Indicates the **rsa_aes_128_cbc_sha** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_CBC to encrypt data, and the SHA algorithm to compute the message authentication code (MAC).	-
rsa_aes_128_sha256	Indicates the **rsa_aes_128_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_CBC to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-
rsa_aes_256_sha256	Indicates the **rsa_aes_256_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 256-bit AES_CBC to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-
rsa_aes128_ccm	Indicates the **rsa_aes128_ccm** cipher suite. This cipher suite uses the RSA algorithm to compute the key and the 128-bit AES_CCM to encrypt data.	-
rsa_aes128_gcm_sha256	Indicates the **rsa_aes128_gcm_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_GCM to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rsa_aes256_ccm	Indicates the **rsa_aes256_ccm** cipher suite. This cipher suite uses the RSA algorithm to compute the key and the 256-bit AES_CCM to encrypt data.	-
rsa_aes256_gcm_sha384	Indicates the **rsa_aes256_gcm_sha384** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 256-bit AES_GCM to encrypt data, and the SHA2-384 algorithm to compute the MAC.	-
ecdhe_rsa_aes128_gcm_sha256	Indicates the **ecdhe_rsa_aes128_gcm_sha256** cipher suite. This cipher suite uses the ECDHE RSA algorithm to compute the key, the 128-bit AES_GCM to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-
ecdhe_rsa_aes256_gcm_sha384	Indicates the **ecdhe_rsa_aes256_gcm_sha384** cipher suite. This cipher suite uses the ECDHE RSA algorithm to compute the key, the 256-bit AES_GCM to encrypt data, and the SHA2-384 algorithm to compute the MAC.	-

Views

Client SSL policy view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A cipher suite consists of a data encryption algorithm, a key exchange algorithm, and a MAC algorithm. During an SSL handshake, an SSL client sends a Client Hello message to notify an SSL server of the SSL protocol version and cipher suites that it supports. The SSL server determines the SSL protocol version and cipher suite used for this communication and sends a Server Hello message to notify the client.

The **prefer-ciphersuite** command configures the cipher suite that the Router can use when it functions as an SSL client.

Configuration Impact

If you run the **prefer-ciphersuite** command multiple times in the same client SSL policy view, only the latest configuration takes effect.

Precautions

To ensure high security, you are not advised to configure the cipher suite used by the client SSL policy to **rsa_3des_cbc_sha** and **rsa_aes_128_cbc_sha**.

Ensure that the cipher suite specified in this command is supported by the SSL server. Before running this command, check the cipher suites that the SSL server supports.

Example

Configure a client SSL policy to use the **rsa_aes_256_sha256** cipher suite.

```
<Huawei> system-view
[Huawei] ssl policy users type client
[Huawei-ssl-policy-users] prefer-ciphersuite rsa_aes_256_sha256
```

Related Topics

19.18.10 ssl policy
19.18.8 server-verify enable
19.18.1 ciphersuite

19.18.6 renegotiation enable

Function

The **renegotiation enable** command enables re-negotiation of an SSL connection.

The **undo renegotiation enable** command disables re-negotiation of an SSL connection.

By default, re-negotiation of an SSL connection is enabled.

Format

renegotiation enable

undo renegotiation enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A client and a server negotiate session parameters by using the SSL handshake protocol to verify the identities of the two parties and negotiate the private key and cipher suite. Asymmetric cryptography is used to encrypt keys and authenticate peer identities when session parameters are being negotiated during the handshake. The computation workload is heavy, consuming a lot of system resources.

If an attacker sends re-negotiation requests continuously, the device consumes a lot of system resources processing these requests. To process re-negotiation requests, a server consumes 15 times the resources that is consumed by a client. This prevents the server from receiving requests from authorized users or suspends the server, affecting normal service operations.

You can run this command to disable re-negotiation of an SSL connection. The device then rejects re-negotiation requests, preventing the preceding problem.

Precautions

After re-negotiation of an SSL connection is disabled, the re-negotiation session will be interrupted.

Example

Disable re-negotiation of an SSL connection on the server.

```
<Huawei> system-view
[Huawei] ssl policy server-users type server
[Huawei-ssl-policy-server-users] undo renegotiation enable
```

Disable re-negotiation of an SSL connection on the client.

```
<Huawei> system-view
[Huawei] ssl policy client-users type client
[Huawei-ssl-policy-client-users] undo renegotiation enable
```

Related Topics

19.18.3 display ssl policy

 Copyright © Huawei Technologies Co., Ltd.

19.18.7 reset ssl connection statistics

Function

The **reset ssl connection statistics** command deletes statistics on SSL connections.

Format

reset ssl connection statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before counting the maximum number of SSL connections within a certain period of time, delete the existing SSL statistics first.

Precautions

SSL statistics cannot be restored after you delete them. So, confirm the action before you use the command.

Example

Delete statistics on SSL connections.

```
<Huawei> reset ssl connection statistics
```

Related Topics

19.18.2 display ssl connection statistics

19.18.8 server-verify enable

Function

Using the **server-verify enable** command, you can enable SSL server authentication in a client SSL policy.

Using the **undo server-verify enable** command, you can disable SSL server authentication in a client SSL policy.

 Copyright © Huawei Technologies Co., Ltd.

By default, SSL server authentication is enabled in a client SSL policy.

Format

server-verify enable

undo server-verify enable

Parameters

None

Views

Client SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSL server and an SSL client perform a handshake to negotiate session parameters and establish a session. During the handshake, the SSL client authenticates the SSL server by checking its digital certificate.

The **server-verify enable** command enables the Router to authenticate SSL servers when it functions as an SSL client.

Precautions

Exercise caution when running the **undo server-verify enable** command because communication becomes insecure after this command is executed.

Example

Enable SSL server authentication.

```
<Huawei> system-view
[Huawei] ssl policy users type client
[Huawei-ssl-policy-users] server-verify enable
```

Related Topics

19.18.10 ssl policy

19.18.4 pki-realm

19.18.9 session

Function

Using the **session** command, you can set the maximum number of sessions that can be saved and the timeout period of a saved session.

 Copyright © Huawei Technologies Co., Ltd.

Using the **undo session** command, you can restore the default configuration.

By default, a maximum of 3600 sessions can be saved, and the timeout period of a saved session is as follows:

- AR100&AR120&AR150&AR160&AR200 series: 32
- AR1200 series: 128
- AR2200 series: 128
- AR3200 series: 256
- AR3600 series: 256

Format

session { **cachesize** *size* | **timeout** *time* } *

undo session { **cachesize** | **timeout** } *

Parameters

Parameter	Description	Value
cachesize *size*	Sets the maximum number of sessions that can be saved on the SSL server.	The value is an integer that varies according to different devices.
timeout *time*	Sets the timeout period of a saved session.	The value is an integer that ranges from 1800 to 72000, in seconds.

Views

Server SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSL server and an SSL client carry out a complex SSL handshake to establish a session. To streamline the SSL handshake process, the SSL protocol allows the server and client to use the previously negotiated parameters to establish new sessions. Therefore, the SSL server must store session information. The **session** command configures the maximum number of sessions that can be saved and the timeout period of a saved session.

- If the number of saved sessions reaches the maximum number, the SSL client stops saving new sessions.

 Copyright © Huawei Technologies Co., Ltd.

- When the timeout period of a session expires, the SSL server deletes the session.

Precautions

If you run the **session** command multiple times in the same server SSL policy view, only the latest configuration takes effect.

Example

Set the maximum number of sessions that can be saved to 50, and the timeout period of a saved session to 7200s.

```
<Huawei> system-view
[Huawei] ssl policy users type server
[Huawei-ssl-policy-users] session cachesize 50 timeout 7200
```

Related Topics

19.18.10 ssl policy

19.18.10 ssl policy

Function

Using the **ssl policy** command, you can create an SSL policy and enter its view, or enter the view of an existing SSL policy.

Using the **undo ssl policy** command, you can delete an SSL policy.

By default, no SSL policy is created.

Format

ssl policy *policy-name* [**type** { **client** | **server** }]

undo ssl policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain any space or question mark (?).
type { **client** | **server** }	Specifies the type of an SSL policy: client SSL policy or server SSL policy.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Secure Sockets Layer (SSL) protocol protects data privacy on the Internet. It allows a client and a server to communicate in a way designed to prevent eavesdropping.

You can use the **ssl policy** command to create a client or server SSL policy, and configure SSL parameters in the SSL policy view.

Precautions

You must set the SSL policy type when creating an SSL policy. To enter the SSL policy view, you only need to specify the policy name.

The device supports a maximum of 16 SSL policies.

To ensure that the functions referencing SSL policy, such as HTTPS, are available by default, a default server SSL policy exists on the Router. The default policy is bound to a default PKI domain.

Example

Create a client SSL policy **users**.

```
<Huawei> system-view
[Huawei] ssl policy users type client
```

Related Topics

19.18.4 pki-realm

19.18.3 display ssl policy

19.18.11 ssl renegotiation-rate

Function

The **ssl renegotiation-rate** command sets the SSL renegotiation rate.

The **undo ssl renegotiation-rate** command restores the SSL renegotiation rate to default value.

By default, the SSL renegotiation is performed once per second.

Format

ssl renegotiation-rate *rate*

 Copyright © Huawei Technologies Co., Ltd.

undo ssl renegotiation-rate

Parameters

Parameter	Description	Value
rate	Specifies how many times SSL renegotiation is performed per second.	The value is an integer that ranges from 0 to 65535. By default, the SSL renegotiation is performed once per second. The value 0 indicates that the SSL renegotiation rate is not limited.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Disabling the renegotiation function on the device can protect the device against renegotiation attacks, but will interrupt services. Therefore, you can keep the renegotiation function enabled, and set the SSL renegotiation rate to minimize the impact of renegotiation attacks on services.

You can set the SSL renegotiation rate according to the CPU capability of the device.

Example

Set the SSL renegotiation rate to 2.

```
<Huawei> system-view
[Huawei] ssl renegotiation-rate 2
```

19.18.12 version (Client SSL policy view)

Function

The **version** command specifies an SSL protocol version in a client SSL policy.

The **undo version** command restores the default SSL protocol version.

By default, a client SSL policy uses Transport Layer Security (TLS) version 1.2.

Format

version { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** }

undo version

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ssl3.0	Indicates that the SSL client uses SSL3.0 to communicate with the SSL server.	-
tls1.0	Indicates that the SSL client uses TLS1.0 to communicate with the SSL server.	-
tls1.1	Indicates that the SSL client uses TLS1.1 to communicate with the SSL server.	-
tls1.2	Indicates that the SSL client uses TLS1.2 to communicate with the SSL server. **NOTE** TLS1.2 version is recommended, other protocol version has potential security risks.	-

Views

Client SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSL server and an SSL client perform a handshake to negotiate session parameters and establish a session. During an SSL handshake, the SSL client sends a Client Hello message to notify the SSL server of the SSL protocol version and cipher suites that it supports. The SSL server determines the SSL protocol version and cipher suite used for this communication and sends a Server Hello message to notify the client.

The **version** command configures the SSL version used by the SSL client. The SSL client sends a Client Hello message to the SSL server to notify the server of the configured SSL version, and the SSL server determines the SSL version used for this communication.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If you run the **version** command multiple times in the same client SSL policy view, only the latest configuration takes effect.

Ensure that the SSL protocol version specified in this command is supported by the SSL server. Before running this command, check the SSL protocol versions that the SSL server supports.

Example

Configure a client SSL policy to use TLS1.1.

```
<Huawei> system-view
[Huawei] ssl policy users type client
[Huawei-ssl-policy-users] version tls1.1
```

Related Topics

19.18.10 ssl policy

19.18.13 version (server SSL policy view)

Function

The **version** command specifies an SSL protocol version in a server SSL policy.

The **undo version** command restores the default SSL protocol versions of the server SSL policy.

By default, a server SSL policy uses Transport Layer Security (TLS) versions 1.2.

Format

version { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** } *

undo version

Parameters

Parameter	Description	Value
ssl3.0	Indicates that the SSL server uses SSL3.0 to communicate with the SSL client.	-
tls1.0	Indicates that the SSL server uses TLS1.0 to communicate with the SSL client.	-
tls1.1	Indicates that the SSL server uses TLS1.1 to communicate with the SSL client.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tls1.2	Indicates that the SSL server uses TLS1.2 to communicate with the SSL client. **NOTE** TLS1.2 version is recommended, other protocol version has potential security risks.	-

Views

Server SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSL client and an SSL server perform a handshake to negotiate session parameters and establish a session. During an SSL handshake, an SSL client sends a Client Hello message to notify an SSL server of the SSL protocol version, encryption algorithm, key exchanging algorithm, and MAC algorithm that it supports. The SSL server determines the SSL protocol version and cipher suite used for this communication and sends a Server Hello message to the client.

The **version** command specifies the SSL protocol version used in the server SSL policy. Then a Server Hello message containing the configured SSL protocol version to the SSL client, and the SSL server determines the SSL protocol version used for this communication.

Precautions

If you run the **version** command multiple times in the same server SSL policy view, only the latest configuration takes effect.

Example

Configure a server SSL policy to use TLS1.1.

```
<Huawei> system-view
[Huawei] ssl policy users type server
[Huawei-ssl-policy-users] version tls1.1
```

Related Topics

19.18.10 ssl policy

 Copyright © Huawei Technologies Co., Ltd.

19.19 HTTPS Configuration Commands

19.19.1 http secure-client ssl-policy

Function

The **http secure-client ssl-policy** command associates a client SSL policy to an HTTPS client.

The **undo http secure-client ssl-policy** command disassociates a client SSL policy from an HTTPS client.

By default, an HTTPS client is not associated with any client SSL policy.

Format

http secure-client ssl-policy *policy-name*

undo http secure-client ssl-policy

Parameters

Message	Description	Value
policy-name	Specifies the name of the client SSL policy to be associated with an HTTPS client.	The value is a string of 1 to 31 case-sensitive characters without spaces or question mark (?).

Views

System view

Default Level

3: Management level

Usage Guidelines

Use Scenario

When the web proxy service of SSL VPN is configured on the device, if the web server only provides HTTPS service, this command is mandatory. The device functioning as the HTTPS client can use the data encryption, identity authentication, and message integrity check mechanisms provided by the SSL protocol to securely transmit data with the web server.

Prerequisites

A client SSL policy has been created using the **ssl policy** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Associate the client SSL policy **users** to the HTTPS client.

```
<Huawei> system-view
[Huawei] http secure-client ssl-policy users
```

Related Topics

19.18.10 ssl policy

19.19.2 http secure-server enable

Function

The **http secure-server enable** command enables the HTTPS server function on the device.

The **undo http secure-server enable** command disables the HTTPS server function on the device.

By default, the HTTPS server function is enabled on the device.

Format

http secure-server enable

undo http secure-server enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When users use the web page to access a remote device functioning as an HTTP server, the following problems exist:

- Users cannot authenticate the device.
- Privacy and integrity of data transmitted between users and the device cannot be ensured.

This command enables the device to function as an HTTPS server. The device uses the SSL protocol's data encryption, identity authentication, and message integrity check mechanisms to protect security of data transmitted between users and the

 Copyright © Huawei Technologies Co., Ltd.

device. These mechanisms ensure that users securely access a remote device on web pages.

Precautions

An SSL policy must have been associated with the HTTPS server using the **http secure-server ssl-policy** command. Otherwise, the **http secure-server ssl-policy** command does not take effect.

Example

Enable the HTTPS server function on the device.

```
<Huawei> system-view
[Huawei] http secure-server enable
```

Related Topics

19.19.4 http secure-server ssl-policy

19.19.3 http secure-server manager-port

Function

The **http secure-server manager-port** command enables the management port of the HTTPS server and sets the management port number.

The **undo http secure-server manager-port** command restores the default setting of the HTTPS server's management port.

By default, the management port of the HTTPS server is disabled.

NOTE

Only users at level 3 and higher levels can log in to the web platform through the management port.

Format

http secure-server manager-port *port-number*

undo http secure-server manager-port

Parameters

Parameter	Description	Value
port-number	Specifies the management port number of the HTTPS server.	The value is 443 or an integer that ranges from 1025 to 51200.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to enable the management port of the HTTPS server and set the management port number, and then can manage the router.

Precautions

Changing the management port number of the HTTPS server forces all online users to go offline. Therefore, exercise caution when performing this operation.

Example

Set the management port number of the HTTPS server to 1066.

```
<Huawei> system-view
[Huawei] http secure-server manager-port 1066
```

19.19.4 http secure-server ssl-policy

Function

The **http secure-server ssl-policy** command applies a server SSL policy to the HTTPS service.

The **undo http secure-server ssl-policy** command cancels the configuration.

By default, the server SSL policy applied to the HTTPS service on the device is default_policy.

Format

http secure-server ssl-policy *policy-name*

undo http secure-server ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a server SSL policy.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain any space or question mark (?).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies a server SSL policy to the HTTPS service. The device functioning as the HTTPS server uses the SSL protocol's data encryption, identity authentication, and message integrity check mechanisms to ensure the security of data transmitted between users and the device.

Prerequisites

A server SSL policy has been created using the **ssl policy** command.

Precautions

After the HTTPS server function is enabled using the **http secure-server enable** command, you cannot change or delete the server SSL policy associated with the HTTPS server. Before changing or deleting the server SSL policy associated with the HTTPS server, run the **undo http secure-server enable** command to disable the HTTPS server function.

Example

Apply a server SSL policy to the HTTPS service.

```
<Huawei> system-view
[Huawei] http secure-server ssl-policy users
```

Related Topics

19.18.10 ssl policy

19.19.5 http secure-server port

Function

Using the **http secure-server port** command, you can set the port number for the HTTPS service.

Using the **undo http secure-server port** command, you can restore the default port number of the HTTPS service.

By default, the port number of the HTTPS service is 443.

Format

http secure-server port *port-number*

undo http secure-server port

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
port-number	Specifies the port number of the HTTPS service.	The value is an integer that ranges from 1025 to 51200. The default value is 443.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the port number of the HTTPS service is 443. Attackers may use the default port to attack an HTTPS server, reducing the bandwidth and deteriorating the performance of the HTTPS server. As a result, authorized users cannot access the HTTPS server.

This command allows you to set another port number for the HTTPS service to avoid such attacks.

Precautions

Changing the port number of the HTTPS service forces all online users to go offline. Therefore, exercise caution when performing this operation.

Example

Set the port number of the HTTPS service to 1278.

```
<Huawei> system-view
[Huawei] http secure-server port 1278
```

Related Topics

19.19.4 http secure-server ssl-policy

19.20 Keychain Configuration Commands

19.20.1 algorithm

 Copyright © Huawei Technologies Co., Ltd.

Function

The **algorithm** command configures a key authentication algorithm.

The **undo algorithm** command deletes a key authentication algorithm.

By default, no algorithm is configured.

Format

algorithm { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** | **simple** }

undo algorithm

Parameters

Parameter	Description	Value
hmac-md5	Indicates that HMAC (Keyed-Hashing for Message Authentication)-Message Digest 5 (MD5) is used for packet encryption and authentication. **NOTE** HMAC-MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
hmac-sha-256	Indicates that HMAC-Secure Hash Algorithm 256 (SHA-256) is used for packet encryption and authentication.	-
hmac-sha1-12	Indicates that HMAC-Secure Hash Algorithm 1-12 (SHA1-12) is used for packet encryption and authentication.	-
hmac-sha1-20	Indicates that HMAC-SHA1-20 is used for packet encryption and authentication.	-
md5	Indicates that MD5 is used for packet encryption and authentication. **NOTE** MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
sha-1	Indicates that SHA-1 is used for packet encryption and authentication. **NOTE** To ensure high security, do not use the SHA-1 algorithm.	-
sha-256	Indicates that SHA-256 is used for packet encryption and authentication.	-
simple	Indicates that the configured key is used for packet authentication. **NOTE** The authentication algorithm specified by **simple** is not secure. HMAC-SHA-256 or SHA-256 is recommended.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. A keychain consists of multiple keys, each of which needs to be configured with an authentication algorithm. Different keys are valid within different time periods, ensuring dynamic change of keychain authentication algorithms.

Packets are authenticated and encrypted based on the authentication algorithm and key string associated with a specified key. This improves the packet transmission security.

The characteristics of each authentication algorithm are as follows:

- MD5: The 128-bit MD5 message digest is calculated based on the entered message of any length.
- SHA-1: The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-MD5: The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length.

  NOTE

  If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message.
- HMAC-SHA-256: The 128-bit SHA-1 message digest.
- HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code.
- HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code.
- SHA-256: The 128-bit SHA-1 message digest.

The MD5 algorithm provides faster calculation speed than the SHA-1 algorithm; the SHA-1 algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA-1, HMAC is more secure, but slower in calculation speed. The HMAC algorithm is recommended to improve data transmission security.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Keys configured on the sender and receiver of packets must correspond to the same authentication and encryption algorithms. Otherwise, packet transmission fails for not passing the authentication.

If algorithm is not configured, key will never be active.

Example

Configure algorithm sha-256 on key-id 1.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1] algorithm sha-256
```

Related Topics

19.20.5 key-id

19.20.6 key-string

19.20.2 default send-key-id

Function

The **default send-key-id** command configures a particular key as the default send key for that keychain.

The **undo default send-key-id** command deletes default send key.

By default, no key is configured as default send key.

Format

default send-key-id

undo default send-key-id

Parameters

None

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key-sting dynamically. This can reduce the workload of changing the algorithm and key manually. A keychain

 Copyright © Huawei Technologies Co., Ltd.

consists of multiple authentication keys, each of which is valid within different time periods. When a key becomes valid, the authentication algorithm corresponding to the key is used, and packets passing the authentication will be sent or received.

If a key for packet sending is not configured in a keychain or no key for packet sending is valid within a certain period, protocol packets cannot be authenticated and encrypted. As a result, protocol packet transmission fails. To address such a problem, configure a default key for packet sending. If no key is valid, the default key for packet sending is used.

Precautions

Each keychain can have only one default key for packet sending.

- If the default key for packet sending is an existing key, the authentication and encryption algorithms, and key corresponding to the key are used.
- If the default key for packet sending is a newly created key, configure the authentication and encryption algorithms.

Example

Configure the key-1 as default send key in keychain huawei.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1] default send-key-id
```

Related Topics

19.20.5 key-id

19.20.3 display keychain

Function

The **display keychain** command displays the configuration of a specified keychain.

Format

display keychain *keychain-name* [**key-id** *key-id*]

Parameters

Parameter	Description	Value
keychain-name	Displays the configuration of a keychain with a specified name.	The keychain must already exist.
key-id *key-id*	Displays the configuration of a specified key in the keychain.	The key must already exist.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

To troubleshoot a keychain authentication failure or collect required information before configuration, run the **display keychain** command to view configurations of a specified keychain.

Example

Display the configuration of the keychain **huawei**.

```
<Huawei> display keychain huawei
 Keychain Information:
 ---------------------
 Keychain Name            : huawei
   Timer Mode             : Absolute
   Time Type              : Utc
   Receive Tolerance(min) : 100
   TCP Kind               : 182
   TCP Algorithm IDs      :
     HMAC-MD5             : 5
     HMAC-SHA1-12         : 2
     HMAC-SHA1-20         : 6
     HMAC-SHA-256         : 7
     SHA-256              : 8
     MD5                  : 3
     SHA1                 : 4
 Number of Key IDs        : 1
 Active Send Key ID       : 1
 Active Receive Key IDs   : 01
 Default send Key ID      : 1
 Default send Key Status  : Inactive

 Key ID Information:
 -------------------
 Key ID                   : 1
   Key string             : ******
   Algorithm              : MD5
   SEND TIMER             :
     Start time           : 2012-03-14 00:00
     End time             : 2012-08-08 23:59
     Status               : Active
   RECEIVE TIMER          :
     Start time           : 2012-03-14 00:00
     End time             : 2012-08-08 23:59
     Status               : Active

 Key ID                   : 2
   Key string             : -
   Algorithm              : -
   SEND TIMER             :
     Status               : Inactive
   RECEIVE TIMER          :
     Status               : Inactive
```

Display the configuration of key-id 1 in the keychain **huawei**.

```
<Huawei> display keychain huawei key-id 1
 Keychain Information:
 ---------------------
 Keychain Name            : huawei
   Timer Mode             : Absolute
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Time Type             : Utc
  Receive Tolerance(min)  : 100
  TCP Kind              : 182
  TCP Algorithm IDs       :
    HMAC-MD5            : 5
    HMAC-SHA1-12          : 2
    HMAC-SHA1-20          : 6
    HMAC-SHA-256          : 7
    SHA-256             : 8
    MD5                 : 3
    SHA1                : 4

Key ID Information:
-------------------
Key ID                : 1
  Key string            : ******
  Algorithm             : MD5
  SEND TIMER              :
    Start time          : 2012-03-14 00:00
    End time            : 2012-08-08 23:59
    Status              : Active
  RECEIVE TIMER           :
    Start time          : 2012-03-14 00:00
    End time            : 2012-08-08 23:59
    Status              : Active
  DEFAULT SEND KEY ID INFORMATION
    Default             : Configured
    Status              : Inactive
```

Table 19-177 Description of the display keychain command output

Item	Description
Keychain Name	Name of a keychain. To set the keychain name, run the **keychain** command.
Timer Mode	Time mode of a keychain. • Absolute: The keychain takes effect in an absolute time range. • Daily periodic: The keychain is valid on a daily basis. • Weekly periodic: The keychain is valid on a weekly basis. • Monthly periodic: The keychain is valid on a monthly basis. • Yearly periodic: The keychain is valid on a yearly basis. To set the time mode, run the **keychain** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Time Type	Time type of a keychain. • Lmt: The time type of Keychain is Local Mean Time (LMT). • Utc: The time type of Keychain is Universal Time Coordinated (UTC). To set the time type, run the **time mode** command.
Receive Tolerance(min)	Receive tolerance time configured for a keychain. To set the receive tolerance time, run the **receive-tolerance** command.
TCP Kind	TCP kind value configured for a keychain. To set the TCP kind value, run the **tcp-kind** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
TCP Algorithm IDs	TCP algorithm ID configured for a keychain. The characteristics of each authentication algorithm are as follows: • MD5: The 128-bit MD5 message digest is calculated based on the entered message of any length. • SHA-1: The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. • HMAC-MD5: The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. **NOTE** If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message. • HMAC-SHA-256: The 128-bit SHA-1 message digest. • HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code. • HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code. • SHA-256: The 128-bit SHA-1 message digest. The MD5 algorithm provides faster calculation speed than the SHA-1 algorithm; the SHA-1 algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA-1, HMAC is more secure, but slower in calculation speed. The HMAC algorithm is recommended to improve data transmission security. To set the TCP algorithm ID, run the **tcp-algorithm-id** command.
Number of Key IDs	Number of key IDs.
Active Send Key ID	ID of the active send key.
Active Receive Key IDs	ID of the active receive key.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default send Key ID	ID of the default send key.
Default send Key Status	Status of the default send key: • Active • Inactive
Key ID	Key configured in a keychain. To set the key ID, run the **key-id** command.
Key string	Key string configured for the key. To set the key string, run the **key-string** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Algorithm	Algorithm configured for the key. The characteristics of each authentication algorithm are as follows: • MD5: The 128-bit MD5 message digest is calculated based on the entered message of any length. • SHA-1: The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. • HMAC-MD5: The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. **NOTE** If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message. • HMAC-SHA-256: The 128-bit SHA-1 message digest. • HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code. • HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code. • SHA-256: The 128-bit SHA-1 message digest. The MD5 algorithm provides faster calculation speed than the SHA-1 algorithm; the SHA-1 algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA-1, HMAC is more secure, but slower in calculation speed. The HMAC algorithm is recommended to improve data transmission security.
SEND TIMER	Send time of a key. To set the send time of a key, run the **send-time** command.
Start time	Time when a key becomes valid.
End time	Time when a key becomes invalid.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Status	Status of send/receive keys: • Active • Inactive
RECEIVE TIMER	Receive time of a key. To set the receive time of a key, run the **receive-time** command.
DEFAULT SEND KEY ID INFORMATION	Information about the default send key.
Default	Configuration of the default send key: • Not configured • Configured
Status	Status of the default send key: • Active • Inactive

19.20.4 keychain

Function

The **keychain** command creates a new set of keychain rules or displays the keychain view.

The **undo keychain** command deletes the keychain configuration.

By default, no keychain is configured.

Format

keychain *keychain-name* **mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } }

undo keychain *keychain-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
keychain-name	Specifies the keychain name. All the applications identify the set of keychain rules by keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
mode	Indicates the time mode of a keychain. **NOTE** • The time mode of a keychain must be specified when a keychain is created. • You do not need to specify the time mode for a created keychain.	-
absolute	Indicates that the given keychain is non-periodic.	-
periodic	Indicates that the given keychain is periodic.	-
daily	Indicates that the given keychain is day-periodic.	-
weekly	Indicates that the given keychain is week-periodic.	-
monthly	Indicates that the given keychain is month-periodic.	-
yearly	Indicates that the given keychain is year-periodic.	-

Views

System view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by dynamically changing the authentication algorithm and key string. This can prevent unauthorized users from obtaining the key string, and authentication and encryption algorithms, and reduce the workload of manually changing the algorithm and key string.

 Copyright © Huawei Technologies Co., Ltd.

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

There are two keychain time modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

Follow-up Procedure

Run the **key-id** command to configure a key. If the key is not configured, the keychain cannot authenticate and encrypt protocol packets.

The time mode of a key must be the same as the time mode of the keychain.

Precautions

A keychain supports a maximum of 64 keys.

The **keychain** *keychain-name* command displays a specific keychain view. If the keychain specified by *keychain-name* does not exist, the **keychain** *keychain-name* command cannot be executed. To create a keychain, run the **keychain** *keychain-name* **mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } } command.

Example

Configure the keychain **huawei** and enter keychain view.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei]
```

Related Topics

19.20.5 key-id

19.20.5 key-id

Function

The **key-id** command creates a new set of key-ids or displays the key-id view.

The **undo key-id** command deletes the key-id configuration.

By default, no key-id is configured.

Format

key-id *key-id*

undo key-id *key-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
key-id	Specifies the key identification number of a keychain.	The integer value ranges from 0 to 63.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key dynamically. This can reduce the workload of manually changing the algorithm and key.

The dynamic change of the keychain authentication algorithm is implemented based on the keys. Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

Follow-up Procedure

After key-id is specified, perform the following operations:

- Run the **algorithm** command to configure an algorithm used by the key.
- Run the **key-string** command to specify a key string.
- Run the **send-time** command to specify the send time of the key.
- Run the **receive-time** command to specify the receive time of the key.

Precautions

A **key-id** represents a key on the device.

A keychain supports 64 keys, but only one key takes effect during one period.

No active key can be used to authenticate and encrypt protocol packets at the intervals of keys. Therefore, run the **default send-key-id** command to specify a default key.

The time mode of the key must be the same as the time mode of Keychain.

Example

Configure key-id 1.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1]
```

Related Topics

19.20.6 key-string
19.20.1 algorithm
19.20.9 send-time
19.20.7 receive-time

19.20.6 key-string

Function

The **key-string** command specifies a key used for keychain authentication.

The **undo key-string** command deletes a key used for keychain authentication.

By default, no key is configured for keychain authentication.

Format

key-string { **plain** *plain-text* | [**cipher**] *cipher-text* }

undo key-string

Parameters

Parameter	Description	Value
plain *plain-text*	Indicates the plain text used for authentication. The configured text will be stored as unencrypted text and displayed as unencrypted text. **NOTE** When configuring an authentication password, select the ciphertext mode because the password is saved in the configuration file as a simple text if you select the plaintext mode, which has a high risk. To ensure device security, change the password periodically.	The value is a string of case-sensitive characters that can be letters or digits. The value is a string of case-sensitive characters ranging from 1 to 255. **NOTE** If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each user name.
cipher	Specifies the cipher key string used for encryption and decryption.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher-text	Indicates the cipher text used for authentication.	The value is a string of case-sensitive characters that can be letters or digits. The authentication password can be a string of 1 to 255 characters in plaintext or a string of 20 to 392 characters in ciphertext. **NOTE** If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each user name.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by dynamically changing the authentication algorithm and key string. This can prevent unauthorized users from obtaining the key string, and authentication and encryption algorithms, and reduce the workload of manually changing the algorithm and key string.

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

Precautions

An authentication key configured in cipher text mode will be also displayed in cipher text mode. Therefore, remember the plaintext key string when configuring the key in cipher text mode.

If the authentication key is not configured, the corresponding key remains in inactive state.

Example

Configure the key string **Huawei@1234**.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1] key-string cipher Huawei@1234
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.20.5 key-id
19.20.1 algorithm

19.20.7 receive-time

Function

The **receive-time** command configures a key as a receive key for the specified interval of time.

The **undo receive-time** command deletes the receive time configuration.

By default, no receive time is configured.

Format

receive-time *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

receive-time daily *start-time* **to** *end-time*

receive-time day { *start-day-name* **to** *end-day-name* | *day-name &<1-7>* }

receive-time date { *start-date-value* **to** *end-date-value* | *date-value &<1-31>* }

receive-time month { *start-month-name* **to** *end-month-name* | *month-name &<1-12>* }

undo receive-time

Parameters

Parameter	Description	Value
start-time	Specifies the start receive time.	In HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specifies the start date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the receive time in minutes.	The value ranges from 1 to 26280000.
infinite	Indicates that the key will be acting as an active receive key forever from the configured start time.	-
to	Indicates a separator.	-
end-time	Specifies the end receive time.	In HH:MM format. The value ranges from 00:00 to 23:59. The end time must be later than the start start.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end-date	Specifies the end date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
daily	Specifies the daily receive time for the given key.	-
day	Specifies the days of the week.	-
start-day-name	Specifies the day of the week to be configured as the start receive day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun.
end-day-name	Specifies the end receive day for the given key.	It can be Tue, Wed, Thur, Fri, Sat, and Sun. The end day must be later than the start day.
day-name &<1-7>	Specifies the day of the week to be configured as the receive day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun. One or more days can be configured.
date	Specifies the date of the month.	-
start-date-value	Specifies the start date of the month to be configured as the receive date for the given key.	The value ranges from 1 to 31.
end-date-value	Specifies the end receive date of the month.	The value ranges from 2 to 31. The end date must be later than the start date.
date-value &<1-31>	Specifies the date of the month to be configured as the receive date for the given key.	The value ranges from 1 to 31. One or more dates can be configured.
month	Specifies the months of the year.	-
start-month-name	Specifies the month of the year to be configured as the start receive month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
end-month-name	Specifies the end receive month. The end month must be greater than the start month.	The end month must be later than the start month. It can be Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
month-name &<1-12>	Specifies the month of the year to be configured as the receive month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. One or more months can be configured.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm and key string. When a key becomes valid, the corresponding authentication algorithm and the key string are used. Configure different keys for packet sending and receiving to be valid within different time periods.

When the system time is within the specified interval, the receive key is in active state.

There are two keychain validity modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

The mode in which receive keys become valid must be the same as that configured for the keychain.

Precautions

Multiple receive keys can be active at the same time. The device will select a key for decryption based on the received packet.

Example

Configure the receive time with the time mode as absolute and range as infinite.

```
<Huawei> system-view
[Huawei] keychain huawei1 mode absolute
[Huawei-keychain-huawei1] key-id 1
[Huawei-keychain-huawei1-keyid-1] receive-time 14:52 2008-10-1 duration infinite
```

Configure the receive time with the time mode as daily.

```
<Huawei> system-view
[Huawei] keychain huawei2 mode periodic daily
[Huawei-keychain-huawei2] key-id 1
[Huawei-keychain-huawei2-keyid-1] receive-time daily 14:52 to 18:10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.20.9 send-time

19.20.8 receive-tolerance

Function

The **receive-tolerance** command sets receive tolerance for all the receive keys in the keychain.

The **undo receive-tolerance** command deletes the receive tolerance configuration.

By default, no receive tolerance is configured.

Format

receive-tolerance { *value* | **infinite** }

undo receive-tolerance

Parameters

Parameter	Description	Value
value	Specifies the receive tolerance value for a keychain.	The integer value ranges from 1 to 14400 in minutes.
infinite	Indicates that the receive tolerance is infinite. That is, the receive key is always valid.	-

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key string dynamically. Each key is configured with an authentication algorithm and a key string. When a key becomes valid, the corresponding authentication algorithm is used.

Due to the networking environment or clock asynchronization on the packet sender and receiver, packets may be delayed. The receiver may receive a packet sent from the sender after its key for packet receiving becomes invalid. As a result, the receiver discards the packet and packet transmission is interrupted. To address this problem, set a tolerance time to ensure that the validity period of the receive

 Copyright © Huawei Technologies Co., Ltd.

key on the receiver expires after all packets sent from the sender reach the receiver.

Precautions

A tolerance time is required for each keychain. The configured tolerance time takes effect for all keys in the keychain.

Example

Configure the receive tolerance time as 570 minutes.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] receive-tolerance 570
```

19.20.9 send-time

Function

The **send-time** command configures a key as a send key at a specified interval.

The **undo send-time** command deletes the send time configuration.

By default, no send-time is configured.

Format

send-time *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

send-time daily *start-time* **to** *end-time*

send-time day { *start-day-name* **to** *end-day-name* | *day-name &<1-7>* }

send-time date { *start-date-value* **to** *end-date-value* | *date-value &<1-31>* }

send-time month { *start-month-name* **to** *end-month-name* | *month-name &<1-12>* }

undo send-time

Parameters

Parameter	Description	Value
start-time	Specifies the start send time.	The value is in HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specify the start date.	The value is in YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the send time, in minutes.	The value ranges from 1 to 26280000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
infinite	Indicates that the key will act as a send key forever from the configured start time.	-
to	Indicates a separator.	-
end-time	Specifies the end send time.	The value is in HH:MM format. The value ranges from 00:00 to 23:59. The end time must be later than the start time.
end-date	Specifies the end date.	The value is in YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
daily	Specifies the daily send time for the given key.	-
day	Specifies the days of the week.	-
start-day-name	Specifies the day of the week to be configured as the start send day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun.
end-day-name	Specifies the end send day for the given key.	It can be Tue, Wed, Thur, Fri, Sat, and Sun. The end day must be later than the start day.
day-name &<1-7>	Specifies the day of the week to be configured as the send day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun. One or more days can be configured.
date	Specifies the date of the month.	-
start-date-value	Specifies the start date of the month to be configured as the send date for the given key.	The value ranges from 1 to 31.
end-date-value	Specifies the end date of the month to be configured as the send date for the given key.	the The value ranges from 2 to 31. The end date must be greater than the start date.
date-value &<1-31>	Specifies the date of the month to be configured as the send date for the given key.	The value ranges from 1 to 31. One or more dates can be configured.
month	Specifies the months of the year.	-
start-month-name	Specifies the month of the year to be configured as the start send month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end-month-name	Specifies the end send month. The end month must be greater than the start month.	It can be Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. The end month must be later than the start month.
month-name &<1-12>	Specifies the month of the year to be configured as the send month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. One or more months can be configured.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm and a key string. When a key becomes valid, the corresponding authentication algorithm and the key string are used. Configure different send and receive keys to be valid within different time periods.

When the system is within the send time range of the key, the device will use the algorithm and key of the configured key to encrypt the packet.

There are two keychain validity modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

The mode in which send keys become valid must be the same as that configured for the keychain.

Precautions

Multiple receive keys cannot be active at the same time. Only one key takes effect during a period in a keychain.

Example

Configure the send time with the time mode as absolute.

```
<Huawei> system-view
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] keychain huawei1 mode absolute
[Huawei-keychain-huawei1] key-id 1
[Huawei-keychain-huawei1-keyid-1] send-time 14:52 2008-10-1 to 14:52 2040-10-1
```

Configure the send time with the time mode as daily.

```
<Huawei> system-view
[Huawei] keychain huawei2 mode periodic daily
[Huawei-keychain-huawei2] key-id 1
[Huawei-keychain-huawei2-keyid-1] send-time daily 14:52 to 18:10
```

Related Topics

19.20.7 receive-time

19.20.10 tcp-algorithm-id

Function

The **tcp-algorithm-id** command specifies a TCP algorithm ID to represent an algorithm supported by the keychain.

The **undo tcp-algorithm-id** command restores the default settings.

By default, mapping between the TCP algorithm and algorithm ID supported by IANA is used.

Format

tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** } *algorithm-id*

undo tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** }

Parameters

Parameter	Description	Value
hmac-md5	Specifies that message authentication algorithm used is HMAC-MD5. **NOTE** HMAC-MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
hmac-sha-256	Specifies that message authentication algorithm used is HMAC-SHA-256.	-
hmac-sha1-12	Specifies that message authentication algorithm used is HMAC-SHA1-12.	-
hmac-sha1-20	Specifies that message authentication algorithm used is HMAC-SHA1-20.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
md5	Specifies that message authentication algorithm used is MD5. **NOTE** MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
sha-1	Specifies that message authentication algorithm used is SHA-1. **NOTE** To ensure high security, do not use the SHA-1 algorithm.	-
sha-256	Specifies that message authentication algorithm used is SHA-256.	-
algorithm-id	Specifies the TCP algorithm ID to represent the algorithm.	The value ranges from 1 to 63. Default algorithm id for algorithm types are: **md5** is 3, **hmac-sha-256** is 7, **sha-1** is 4, **hmac-md5** is 5, **hmac-sha1-12** is 2, **hmac-sha1-20** is 6 and **sha-256** is 8.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. Packets to be transmitted over non-TCP and TCP connections are authenticated using authentication and encryption algorithms and key string corresponding to a key. The TCP connection needs to be authenticated to enhance security.

The TCP connection is authenticated using the authentication algorithm specified by the algorithm ID. The algorithm ID is not defined by IANA. Different vendors use different algorithm IDs to identify authentication algorithms. When two devices of different vendors are connected, ensure that algorithm IDs configured on the two devices are the same.

The characteristics of each authentication algorithm are as follows:

- MD5: The 128-bit MD5 message digest is calculated based on the entered message of any length.

 Copyright © Huawei Technologies Co., Ltd.

- SHA-1: The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-MD5: The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length.

  NOTE

  If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message.
- HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code.
- HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code.

Follow-up Procedure

After configuring algorithm IDs for the communicating parties, run the **tcp-kind** command to configure TCP types for the communicating parties.

Precautions

Each algorithm has a unique algorithm ID.

Example

Configure the TCP algorithm ID of **hmac-sha-256** as 1.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] tcp-algorithm-id hmac-sha-256 1
```

Related Topics

19.20.11 tcp-kind

19.20.11 tcp-kind

Function

The **tcp-kind** command specifies the option type in the TCP enhanced authentication option.

The **undo tcp-kind** command restores the default TCP kind value.

By default, the default kind value is 254.

Format

tcp-kind *kind-value*

undo tcp-kind

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
kind-value	Specifies the TCP kind value to be used for that keychain.	The value ranges from 28 to 255.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. Packets to be transmitted over non-TCP and TCP connections are authenticated using authentication and encryption algorithms and key string corresponding to a key. The TCP connection needs to be authenticated to enhance security.

TCP connection request packets carry enhanced authentication options and are authenticated by a specified authentication algorithm. Different vendors use different kind values to specify the enhanced authentication option. Kind values configured for the communicating parties must be the same.

Follow-up Procedure

After configuring the same TCP kind value for the communicating parties, run the **tcp-algorithm-id** command to specify TCP algorithm IDs for the communicating parties.

Precautions

Communicating parties using the keychain authentication must establish a TCP connection when configuring the kind value. Otherwise, the TCP authentication does not take effect.

Example

Configure the TCP kind value as 252 for the keychain **huawei**.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] tcp-kind 252
```

Related Topics

19.20.4 keychain

19.20.10 tcp-algorithm-id

 Copyright © Huawei Technologies Co., Ltd.

19.20.12 time mode

Function

The **time mode** command configures the time mode for Keychain.

The **undo time mode** command restores the default time mode for Keychain.

By default, the time mode of Keychain is Local Mean Time (LMT).

Format

time mode { **utc** | **lmt** }

undo time mode

Parameters

Parameter	Description	Value
utc	Specifies that the configured time is in Universal Time Coordinated (UTC) format.	-
lmt	Specifies that the configured time is in LMT format.	-

Views

Keychain view

Default Level

2: Configuration level

Usage Guidelines

Each keychain consists of multiple key IDs that are valid within different time periods and each key ID is configured with an authentication algorithm. When a key ID becomes valid, the corresponding authentication algorithm is used, ensuring the dynamic change of authentication algorithms. Configure different key IDs for packet sending and receiving to be valid within different time periods.

To configure the time mode for Keychain, run the **time mode** command. You can configure UTC or LMT for Keychain based on the network planning. Ensure that the time mode remains the same on the entire network.

Example

Configure the time mode for Keychain as UTC.

```
<Huawei> system-view
[Huawei] keychain huawei1 mode absolute
[Huawei-keychain-huawei1] time mode utc
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.20.4 keychain

 Copyright © Huawei Technologies Co., Ltd.