11 WLAN-AC Commands

11.1 WLAN Service Configuration Commands

11.1.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.1.2 ac sysnetid

Function

The **ac sysnetid** command configures an NE name for an AC.

The **undo ac sysnetid** command deletes the NE name of an AC.

By default, no NE name is configured for an AC.

Format

ac sysnetid *ac-sysnetid*

undo ac sysnetid

Parameters

Parameter	Description	Value
ac-sysnetid	Specifies the NE name of an AC.	The value is a string of 1 to 32 case-sensitive characters. The value beginning and ending with double quotation marks (" ") can contain spaces. The value can contain digits, letters, and special characters such as the asterisk (*) and number sign (#).

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The administrator can run the **ac sysnetid** command to configure a unique NE name for an AC. This facilitates AC management.

Configuration Impact

If you run the **ac sysnetid** command multiple times, only the latest configuration takes effect.

Example

Set the NE name of an AC to **ABC123**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac sysnetid ABC123
```

11.1.3 active-dull-client enable

Function

The **active-dull-client enable** command enables the function of preventing terminals from entering the power-saving mode.

The **undo active-dull-client enable** command disables the function.

By default, the function of preventing terminals from entering the power-saving mode is disabled.

Format

active-dull-client enable

undo active-dull-client enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to individual reasons, some terminals may not run services normally when entering the power-saving mode. You can run the **active-dull-client enable**

command to enable the function of preventing terminals from entering the power-saving mode. After that, an AP frequently sends QoS data frames to these terminals to prevent them from entering the power-saving mode, ensuring normal services. This function does not take effect for some terminals and cannot prevent the terminals from entering the power-saving mode. For details, see *Test Report on Terminal Compatibility*.

Precautions

After the function is enabled, the terminals consume more power and extra bandwidth. If no terminal unexpectedly enters the power-saving state, you are advised to disable the function.

Example

Enable the function of preventing terminals from entering the power-saving mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] active-dull-client enable
```

11.1.4 active-dull-client force enable

Function

The **active-dull-client force enable** command enables the function of forcibly preventing terminals from entering the power-saving mode.

The **undo active-dull-client force enable** command disables the function of forcibly preventing terminals from entering the power-saving mode.

By default, the function of forcibly preventing terminals from entering the power-saving mode is disabled.

Format

active-dull-client force enable

undo active-dull-client force enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of preventing terminals from entering the power-saving mode is enabled, some special terminals still enter the power-saving mode, causing service packet loss. In this case, you can enable the function of forcibly preventing terminals from entering the power-saving mode to wake up these terminals and prevent them from entering the power-saving mode.

Precautions

Enabling this function increases terminal power consumption and occupies extra bandwidth. Therefore, it is recommended that this function be enabled only when there are such special terminals.

Example

Enable the function of forcibly preventing terminals from entering the power-saving mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] active-dull-client force enable
```

11.1.5 advertise-ap-name enable

Function

The **advertise-ap-name enable** command enables Beacon frames to carry the AP name.

The **undo advertise-ap-name enable** disables Beacon frames from carrying the AP name.

By default, Beacon frames do not carry the AP name.

Format

advertise-ap-name enable

undo advertise-ap-name enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

In certain scenarios, you can run the **advertise-ap-name enable** command to enable Beacon frames to carry the AP name. In this way, you can quickly locate and identify APs by identifying the AP name carried in an SSID or display the AP name on STAs that can receive and resolve the host name carried in SSIDs of multiple APs.

Example

Enable Beacon frames to carry the AP name in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] advertise-ap-name enable
```

11.1.6 agile-antenna-polarization

Function

The **agile-antenna-polarization enable** command enables self-adaptive polarization for agile antennas.

The **undo agile-antenna-polarization enable** command disables self-adaptive polarization for agile antennas.

By default, self-adaptive polarization is disabled for agile antennas.

Format

agile-antenna-polarization enable

undo agile-antenna-polarization enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Self-adaptive polarization for agile antennas can reduce interference between transmit signals of antennas, and increase the transmit power of antennas and the demodulation SNR of STAs. When providing wireless coverage, you can enable this function when the following types of STA exist:

- STA with one transmit antenna and one receive antenna in 1x1 mode
- STA with two transmit antennas and two receive antennas in 2x2 mode

After this function is enabled, the AP uses two mutually orthogonal antennas to communicate with STAs but not a third antenna.

Prerequisites

Dual-polarized antennas have been connected to radio ports A and B on the same frequency band.

Example

Enable self-adaptive polarization for agile antennas in a 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] agile-antenna-polarization enable
```

11.1.7 antenna-gain

Function

(AP group radio view) The **antenna-gain** command configures the antenna gain for all specified AP radios in an AP group.

(AP group radio view) The **undo antenna-gain** command restores the default antenna gain of all specified AP radios in an AP group.

(AP radio view) The **antenna-gain** command configures the antenna gain for an AP radio.

(AP radio view) The **undo antenna-gain** command restores the antenna gain of an AP radio to that configured in the AP group radio view.

By default, no antenna gain is configured for AP radios. The antenna gains of AP radios depend on AP types and operating channels of AP radios. To check the default antenna gains of radios on different AP types, run the **display ap-type** { **id** *type-id* | **type** *ap-type* } command.

Format

antenna-gain *antenna-gain*

undo antenna-gain

Parameters

Parameter	Description	Value
antenna-gain	Specifies the antenna gain.	The value is an integer that ranges from –10 to +30, in dB.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The antenna gain is the ratio of the power density produced by an antenna to the power density that should be obtained at the same point if the power accepted by the antenna were radiated equally. It can measure the capability for an antenna to receive and send signals in a specified direction, which is one of the most important parameters to select a BTS antenna. Under the same condition, a higher antenna gain indicates a longer transmission distance.

Precautions

- The regulatory requirements for the strength of radio signals vary in different countries and regions. Therefore, when APs and external antennas are used together, run the **antenna-gain** command to set the antenna gain based on the actual antenna specifications. Then the device software controls the transmit power based on the configured antenna gain within the range allowed by the country code.
- The antenna gain of an AP radio configured using the command takes effect only for external antennas.
- The maximum transmit power of a radio must comply with local laws and regulations. For details, see *WLAN Country Codes and Channels Compliance*. You can obtain this table at Huawei technical support website.
  - Enterprise technical support website: **https://support.huawei.com/enterprise**
  - Carrier technical support website: **https://support.huawei.com**
- The configuration in the AP radio view has a higher priority than that in the AP group radio view.
- When the antenna gain of an AP is not an integer, the AC rounds the value off and delivers the integer antenna gain. For example, if the 2.4 GHz antenna gain of an AP is 2.5 dB, the 2.4 GHz antenna gain of 3 dB is displayed on the AC.

Example

Set the antenna gain of radio 0 on AP 1 to 4.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] antenna-gain 4
```


11.1.8 ap auth-mode

Function

The **ap auth-mode** command configures the AP authentication mode.

The **undo ap auth-mode** command restores the default AP authentication mode.

By default, the AP authentication mode is MAC address authentication. In the CloudCampus Solution, for an AC in NETCONF mode, the AP authentication mode is SN authentication.

Format

ap auth-mode { **mac-auth** | **no-auth** | **sn-auth** }

undo ap auth-mode

Parameters

Parameter	Description	Value
mac-auth	Indicates the MAC address authentication mode.	-
no-auth	Indicates the none authentication mode.	-
sn-auth	Indicates the SN authentication mode.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After this command is executed, the device authenticates APs using the configured mode.

NOTE

The none authentication mode brings security risks. You are advised to set the authentication mode to MAC address or SN authentication, which is more secure.

Example

Set the AP authentication mode to MAC address authentication.

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



```
[HUAWEI-wlan-view] ap auth-mode mac-auth
Warning: The authentication mode is switched to MAC address authentication. Ensu
re that the APs added offline have MAC address information. Otherwise, configura
tions of these APs may be lost after the device restarts. Continue? [Y/N]:Y
```

11.1.9 ap blacklist

Function

The **ap blacklist** command adds APs to the AP blacklist.

The **undo ap blacklist** command deletes APs from the AP blacklist.

By default, no APs exist in the AP blacklist.

Format

ap blacklist mac *ap-mac1* [**to** *ap-mac2*]

undo ap blacklist mac { *ap-mac1* [**to** *ap-mac2*] | **all** }

Parameters

Parameter	Description	Value
mac *ap-mac1*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
to *ap-mac2*	Specifies the end MAC address during the batch operation. The value of *ap-mac2* must be larger than *ap-mac1*, and *ap-mac1* and *ap-mac2* together specify a range. A maximum of 128 MAC addresses are supported during the batch operation.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
all	Deletes all MAC addresses from the blacklist.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

APs in the blacklist cannot go online. Online APs will be disconnected after it is blacklisted.

Precautions

The AP blacklist and whitelist can both be configured. However, the MAC address of an AP cannot be added to both of them.

If the AP whitelist and blacklist are both configured, the system checks an AP against the blacklist first.

Example

Add the AP with the MAC address of 00e0-fc07-8280 to the AP blacklist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap blacklist mac 00e0-fc07-8280
```

Add MAC addresses from 00e0-fc07-8270 to 00e0-fc07-8276 to the AP blacklist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap blacklist mac 00e0-fc07-8270 to 00e0-fc07-8276
```

11.1.10 ap data-collection enable

Function

The **ap data-collection enable** command enables the AP data caching function.

The **undo ap data-collection enable** command disables the AP data caching function and clears cached data.

By default, the AP data caching function is disabled.

Format

ap data-collection enable

undo ap data-collection enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AC needs to query performance statistics (such as AP and radio performance statistics, and STA association information on APs) from APs. The **ap data-collection enable** command can enable an AC to periodically query data on APs and cache obtained data. Upon the next data query, the AC can directly search for cached data without the need to wait for APs to return data. This greatly reduces timeout for querying AP-related statistics.

If there are a large number of APs and STAs on the AC, this function may occupy many memory resources and affect performance. Therefore, it is recommended that this function be disabled when statistics query is not required.

Precautions

After the **undo ap data-collection enable** command is executed, data of all APs is cleared. However, common Fit APs periodically report performance statistics. Therefore, even if the data cached on the device is cleared, the data can be queried after the APs periodically report data.

Example

Enable the AP data caching function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap data-collection enable
```

11.1.11 ap data-collection interval

Function

The **ap data-collection interval** command sets the AP data buffer duration.

The **undo ap data-collection interval** command restores the default AP data buffer duration.

By default, the device buffers AP data for 5 minutes.

Format

ap data-collection interval *interval*

undo ap data-collection interval

Parameters

Parameter	Description	Value
interval	Specifies the buffer duration.	The value is an integer that ranges from 5 to 60, in minutes.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the AP buffer duration on the device.

Example

Enable the device to buffer AP data and set the buffer duration.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap data-collection enable
[HUAWEI-wlan-view] ap data-collection interval 57
```

11.1.12 ap modify

Function

The **ap modify** command changes information about an AP.

Format

ap modify *ap-id* **mac** *ap-mac*

Parameters

Parameter	Description	Value
ap-id	Specifies the ID of the AP to be replaced.	The AP ID must exist.
mac *ap-mac*	Specifies the MAC address of a new AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When AP hardware needs to be replaced, you can configure new AP information for an existing AP ID to prevent repetitive data configurations. In this way, the new

AP goes online using the ID of the original AP so that all data configurations of the original AP directly take effect on the new AP.

By default, you can run the **display ap** command to view the MAC address of an AP.

Precautions

This configuration enables the new AP to go online on the AC and interrupts services of the original AP.

The type of the new AP must be the same as that of the original AP.

Example

Specify the MAC address **00e0-fc12-3456** of a new AP for the AP ID 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap modify 0 mac 00e0-fc12-3456
Warning: Modify AP will influence the service that has published in AP, Whether to continue? [Y/N]y
```

11.1.13 ap rtu load

Function

The **ap rtu load** command unzips a right-to-use (RTU) license package and automatically delivers the unzipped RTU licenses to the corresponding APs.

NOTE

The RTU License is not supported by the following models.

- AirEngine x76x (Excluding the AirEngine 5760-51, AirEngine 6760-X1, AirEngine 6760-X1E)
- AirEngine x77x
- The cemtral AP (including matching RUs)
- AirEngine 9700D-S (including matching ORUs)

Format

ap rtu load filename *filename*

Parameters

Parameter	Description	Value
filename *filename*	Specifies the name of an RTU license package.	The value is a string of 1 to 64 case-sensitive characters. The package must be a .zip package and have the same name as the existing RTU license package.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

RTU is an authorization mode for selling hardware capabilities in installments, such as the number of spatial streams, capacity, and ports. An RTU license cannot be migrated after being bound to a device. As a part of hardware value, RTU licenses have the same lifecycle and the same entitlement as the hardware. The quantities of spatial streams, antennas, and service ports have always been the indicators for a WLAN in the industry, among which the quantity of spatial streams is the most basic indicator. RTU licensing allows basic AP models to support features such as dual-band, three-radio, and independent scanning radio.

After applying for RTU licenses in batches, you will obtain an RTU license package. You need to manually upload the RTU license package to the AC, and then run this command to unzip the package and automatically deliver the RTU licenses to the corresponding APs.

Prerequisites

An RTU license package has been manually uploaded to the AC.

Configuration Impact

Executing this command will unzip the RTU license package locally on the device, with a list of RTU license files generated.

Precautions

To ensure that RTU-granted functions work properly, license files in the RTU license package must meet the following requirements:

- License files are .dat files downloaded from the Electronic Software Delivery Platform (ESDP).
- The name of a license file (including the file name extension) cannot exceed 64 characters.

Follow-up Procedure

Manually restart the APs to which the RTU licenses have been delivered so that these licenses can take effect.

Example

Unzip an RTU license package and automatically deliver the unzipped RTU licenses to the corresponding APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap rtu load filename rtu.zip
Info: This operation may take a few seconds. Please wait for a moment....done.
Info: Valid license file(s):2048, invalid license file(s):0
Warning: After the RTU file is downloaded to the AP, restart the AP to make RTU take effect.
```


11.1.14 ap whitelist

Function

The **ap whitelist** command adds APs to the AP whitelist.

The **undo ap whitelist** command deletes APs from the AP whitelist.

By default, no APs exist in the AP whitelist.

Format

ap whitelist { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }

undo ap whitelist { **mac** { *ap-mac1* [**to** *ap-mac2*] | **all** } | **sn** { *ap-sn1* [**to** *ap-sn2*] | **all** } }

Parameters

Parameter	Description	Value
mac *ap-mac1*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a 4-digit hexadecimal number.
to *ap-mac2*	Specifies the end MAC address during the batch operation. The value of *ap-mac2* must be larger than *ap-mac1*, and *ap-mac1* and *ap-mac2* together specify a range.	The value is in H-H-H format. An H is a 4-digit hexadecimal number.
sn *ap-sn1*	Specifies the SN of an AP.	The value is a string of 1 to 31 characters.
to *ap-sn2*	Specifies the end SN during the batch operation. The value of *ap-sn2* must be larger than *ap-sn1*, and *ap-sn1* and *ap-sn2* together specify a range.	The value is a string of 1 to 31 characters.
mac all	Deletes all MAC addresses from the whitelist.	-
sn all	Deletes all SNs from the whitelist.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- In MAC address authentication mode configured using the **ap auth-mode** command, if the MAC address of an AP exists in the whitelist, the AP automatically goes online, without the need of manual confirmation. If the MAC address of an AP is not in the whitelist and the AP has not been imported, the AP cannot automatically go online. In this case, you need to run the **ap-confirm** command to confirm the AP.
- When the AP authentication mode is set to SN authentication using the **ap auth-mode** command, if the SN of an online AP exists in the whitelist, the AP automatically goes online, without the need of manual confirmation. If the SN of an AP is not in the whitelist and the AP has not been imported, the AP cannot automatically go online. In this case, you need to run the **ap-confirm** command to confirm the AP.

Prerequisites

The AP authentication mode has been set to MAC address or SN authentication using the **ap auth-mode** command.

Precautions

When adding multiple SNs to the whitelist, ensure that the start SN length and the end SN length are the same.

Example

Add the AP with the MAC address of 00e0-fc07-8280 to the AP whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist mac 00e0-fc07-8280
```

Add MAC addresses from 00e0-fc07-8270 to 00e0-fc07-8290 to the AP whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist mac 00e0-fc07-8270 to 00e0-fc07-8290
```

Add the SN 08PE56430071 to the AP whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist sn 08PE56430071
```

Add SNs from 08PE56430076 to 08PE56430081 to the AP whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist sn 08PE56430076 to 08PE56430081
```

11.1.15 ap-confirm

Function

The **ap-confirm** command confirms unauthenticated APs and allows them to go online.

Format

ap-confirm { **all** | **mac** *ap-mac* | **sn** *ap-sn* }

Parameters

Parameter	Description	Value
all	Confirms all APs.	-
mac *ap-mac*	Confirms the AP with the specified MAC address.	The value is in H-H-H format. An H is a 4-digit hexadecimal number.
sn *ap-sn*	Confirms the AP with the specified SN.	The value is a string of 1 to 31 characters.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After viewing unauthenticated APs using the **display ap unauthorized record** command, you can run the **ap-confirm** command to confirm these unauthenticated APs if you want to connect them to the AC. After confirmation, the APs are allowed to go online, automatically added to the default region, and bound to the default AP profiles.

Example

Confirm the AP with the MAC address 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-confirm mac 00e0-fc12-3456
```

Confirm all APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-confirm all
```

11.1.16 ap-id

Function

The **ap-id** command imports an AP or displays the AP view.

By default, no AP is imported.

Format

ap-id *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }]

Parameters

Parameter	Description	Value
ap-id	Specifies an AP ID.	The value is an integer that ranges from 0 to 1023.
type-id *type-id*	Specifies an AP type ID.	The value is an integer that ranges from 0 to .
ap-type *ap-type*	Specifies an AP type.	The value is a string of 1 to 31 characters.
ap-mac *ap-mac*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
ap-sn *ap-sn*	Specifies an AP SN.	The value is a string of 1 to 31 characters, and can only contain letters and digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to set parameters for an AP imported successfully before it goes online. The parameter settings then take effect when the AP goes online.

To delete an AP, run the **undo ap** command.

Precautions

To add an AP, you must enter the MAC address, SN, or MAC address+SN of the AP. In MAC address authentication mode, enter the MAC address of the AP. In SN authentication mode, enter the SN of the AP.

To enter the AP view, you only need to enter the AP ID.

Example

Import an AP with the ID of 11, type ID of 125, and MAC address of 00e0-fc07-8270.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 11 type-id 125 ap-mac 00e0-fc07-8270
```

11.1.17 ap-mac

Function

The **ap-mac** command imports an AP or displays the AP view.

By default, no AP is imported.

Format

ap-mac *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*]

Parameters

Parameter	Description	Value
ap-mac	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
type-id *type-id*	Specifies an AP type ID.	The value is an integer that ranges from 0 to .
ap-type *ap-type*	Specifies an AP type.	The value is a string of 1 to 31 characters.
ap-id *ap-id*	Specifies an AP ID.	The value is an integer that ranges from 0 to 1023.
ap-sn *ap-sn*	Specifies an AP SN.	The value is a string of 1 to 31 characters, and can only contain letters and digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to set parameters for an AP imported successfully before it goes online. The parameter settings then take effect when the AP goes online.

Precautions

When importing an AP, you must enter the MAC address of the AP. If the AP authentication mode is SN authentication, you also need to enter the SN of the AP.

To enter the AP view, you only need to enter the MAC address of the AP. If the specified MAC address does not exist, the system adds a new AP and displays the AP view.

The **ap-mac** *ap-mac* [[**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*]] and **ap-id** *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }] commands have the same function. You can use either one according to the actual situation.

Example

Import the AP with the MAC address of 00e0-fc07-8260.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-mac 00e0-fc07-8260
```

11.1.18 association-timeout

Function

The **association-timeout** command configures the association aging time for STAs.

The **undo association-timeout** command restores the default association aging time of STAs.

By default, the association aging time of STAs is 5 minutes.

Format

association-timeout *association-timeout*

undo association-timeout

Parameters

Parameter	Description	Value
association-timeout	Specifies the association aging time of STAs.	The value is an integer that ranges from 1 to 30, in minutes.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The administrator can run this command to set the association aging time for STAs. If the AP receives no data packet from a STA in a specified time, the STA goes offline after the association aging time expires.

Precautions

Changing the association aging time of a STA may interrupt the STA services.

Example

Set the association aging time of STAs to 15 minutes in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] association-timeout 15
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.19 auto-off service

Function

The **auto-off service** command enables the scheduled VAP auto-off function and sets the time range within which the VAP is disabled.

The **undo auto-off service** command disables the scheduled VAP auto-off function.

By default, the scheduled VAP auto-off function is disabled.

Format

auto-off service start-time *start-time* **end-time** *end-time*

undo auto-off service

Parameters

Parameter	Description	Value
start-time *start-time*	Specifies the time when a VAP starts to be disabled.	The time is in hh:mm:ss format. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59.
end-time *end-time*	Specifies the time when a VAP stops being disabled.	The time is in hh:mm:ss format. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59.

Views

VAP profile view, 2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an enterprise does not want employees to access the internal WLAN from 01:00 to 05:00, the administrator can run the **auto-off service** command to enable the scheduled VAP auto-off function.

Precautions

- After the service mode of a VAP is enabled using the **undo service-mode disable** command, you can run the **auto-off service** command to configure the scheduled VAP auto-off function. In the scheduled time, the VAP is disabled and cannot be enabled using the **undo service-mode disable** command. To enable the VAP, run the **undo auto-off service** command.
- The scheduled VAP auto-off function takes effect in the scheduled time only after the **undo service-mode disable** command is executed. If the service mode of a VAP is disabled using the **service-mode disable** command, the VAP auto-off function does not take effect.

- The scheduled VAP auto-off function enabled in a VAP profile view takes effect only on the APs using the VAP profile, and the scheduled VAP auto-off function enabled in a radio profile view takes effect only on the APs using the radio profile.

Example

Configure the scheduled VAP auto-off function in the VAP profile **vap1**, and configure the VAP to be disabled from 1:00:00 to 7:00:00.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] auto-off service start-time 1:00:00 end-time 7:00:00
```

11.1.20 beacon-2g-rate

Function

The **beacon-2g-rate** command sets the transmit rate of 2.4 GHz management frames (including Beacon frames, Probe Response frames, Assoc/Reassoc Response frames, and Auth frames).

The **undo beacon-2g-rate** command restores the default transmit rate of 2.4 GHz management frames.

By default, the transmit rate of 2.4 GHz management frames is 5.5 Mbit/s.

Format

beacon-2g-rate *beacon-2g-rate*

undo beacon-2g-rate

Parameters

Parameter	Description	Value
beacon-2g-rate	Specifies the transmit rate of management frames.	The value is of the enumerated type: • 1: 1 Mbit/s • 2: 2 Mbit/s • 5.5: 5.5 Mbit/s • 6: 6 Mbit/s • 9: 9 Mbit/s • 11: 11 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s

Views

SSID profile view, Mesh profile view, WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many management frames occupy a large number of wireless resources. To reduce wireless resource occupation of management frames and improve channel utilization, you can run the **beacon-2g-rate** command to set a high transmit rate for 2.4 GHz management frames.

Precautions

The 802.11b protocol supports only 1 Mbit/s, 2 Mbit/s, 5.5 Mbit/s, and 11 Mbit/s. If you set the transmit rate of management frames to a rate not supported by the 802.11b protocol, STAs supporting only 802.11b cannot connect to the wireless network.

If you run the **radio-type dot11b** command in the 2G radio profile view to set the radio type to **dot11b**, and the 2G radio profile is applied to an AP, *beacon-2g-rate* that takes effect on the 2 GHz radio of the AP is fixed as 1 Mbit/s, and *beacon-2g-rate* configured in the SSID profile view does not take effect on the AP.

Example

Set the transmit rate of 2.4 GHz management frames to 18 Mbit/s in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] beacon-2g-rate 18
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.21 beacon-5g-rate

Function

The **beacon-5g-rate** command sets the transmit rate of 5 GHz management frames (including Beacon frames, Probe Response frames, Assoc/Reassoc Response frames, and Auth frames).

The **undo beacon-5g-rate** command restores the default transmit rate of 5 GHz management frames.

By default, the transmit rate of 5 GHz management frames is 6 Mbit/s.

Format

beacon-5g-rate *beacon-5g-rate*

undo beacon-5g-rate

Parameters

Parameter	Description	Value
beacon-5g-rate	Specifies the transmit rate of management frames.	The value is of the enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s

Views

SSID profile view, Mesh profile view, WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many management frames occupy a large number of wireless resources. To reduce wireless resource occupation of management frames and improve channel utilization, you can run the **beacon-5g-rate** command to set a high transmit rate for 5 GHz management frames.

Example

Set the transmit rate of 5 GHz management frames to 18 Mbit/s in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] beacon-5g-rate 18
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.22 beacon-6g-rate

Function

The **beacon-6g-rate** command sets the transmit rate of 6 GHz management frames (including Beacon frames, Probe Response frames, Assoc/Reassoc Response frames, and Auth frames).

The **undo beacon-6g-rate** command restores the default transmit rate of 6 GHz management frames.

By default, the transmit rate of 6 GHz management frames is 6 Mbit/s.

Format

beacon-6g-rate *beacon-6g-rate*

undo beacon-6g-rate

Parameters

Parameter	Description	Value
beacon-6g-rate	Specifies the transmit rate of management frames.	The value is of the enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s

Views

SSID profile view, Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many management frames occupy a large number of wireless resources. To reduce wireless resource occupation of management frames and improve channel utilization, you can run the **beacon-6g-rate** command to set a high transmit rate for 6 GHz management frames.

Example

Set the transmit rate of 6 GHz management frames to 18 Mbit/s in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] beacon-6g-rate 18
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.23 beacon-interval

Function

The **beacon-interval** command sets the interval for sending Beacon frames.

The **undo beacon-interval** command restores the default interval for an AP to send Beacon frames.

By default, the interval for sending Beacon frames is 100 TUs.

Format

beacon-interval *beacon-interval*

undo beacon-interval

Parameters

Parameter	Description	Value
beacon-interval	Specifies the interval for sending Beacon frames.	The value is an integer that ranges from 60 TUs to 1000 TUs. TU is a time unit equal to 1024 microseconds.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

An AP broadcasts Beacon frames at intervals to notify STAs of an existing 802.11 network. After receiving a Beacon frame, a STA can modify parameters used to connect to the 802.11 network.

A long interval for sending Beacon frames lengthens the dormancy time of STAs, while a short interval for sending Beacon frames increases air interface costs. Therefore, you are advised to set the interval for sending Beacon frames for an AP based on the VAP quantity. The following intervals for sending Beacon frames are recommended for APs with different VAP quantities on a single radio:

- No more than 4 VAPs: about 100 TUs
- 5 to 8 VAPs: about 200 TUs
- 9 to 12 VAPs: about 300 TUs
- 13 to 16 VAPs: about 400 TUs

Ensure that the air scan interval meets the following condition: scan-interval ≥ beacon-interval + 100 ms

Example

Set the interval for sending Beacon frames to 200 TUs in the 2G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] beacon-interval 200
```

11.1.24 beamforming disable

Function

The **beamforming disable** command disables the beamforming function.

The **undo beamforming disable** command enables the beamforming function.

By default, the beamforming function is enabled.

NOTE

This configuration takes effect only on APs running V200R019C10 or later.

Format

beamforming disable

undo beamforming disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Beamforming is a signal processing technique that controls signal transmission direction, and transmission and reception of radio signals. The transmit end uses weight to transmit signals. The signals are transmitted to the destination as narrow beams. Beamforming increases the demodulation signal-to-noise ratio (SNR) for the destination device.

Precautions

If nodes on a Mesh network are fixed and distant from each other, enable the beamforming function to increase the demodulation SNR of Mesh links. Mobile nodes may cause a low demodulation SNR of Mesh links in Mesh scenarios. Therefore, it is recommended that the beamforming function be disabled.

To use the MU-MIMO function, enable the beamforming function.

Example

Disable the beamforming function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] beamforming disable
```

11.1.25 beamforming enable

Function

The **beamforming enable** command enables the beamforming function.

The **undo beamforming enable** command disables the beamforming function.

By default, the beamforming function is disabled.

NOTE

This configuration takes effect only on APs running V200R019C00 or earlier.

Format

beamforming enable

undo beamforming enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Beamforming is a signal processing technique that controls signal transmission direction, and transmission and reception of radio signals. The transmit end uses weight to transmit signals. The signals are transmitted to the destination as narrow beams. Beamforming increases the demodulation signal-to-noise ratio (SNR) for the destination device.

Precautions

If nodes on a WDS or Mesh network are fixed and distant from each other, enable the beamforming function to increase the demodulation SNR of WDS or Mesh links. Mobile nodes may cause a low demodulation SNR of WDS or Mesh links in WDS or Mesh scenarios. Therefore, it is recommended that the beamforming function be disabled.

Example

Enable the beamforming function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] beamforming enable
```

11.1.26 capwap control-link-priority

Function

The **capwap control-link-priority** command configures the priority of CAPWAP management packets.

The **undo capwap control-link-priority** command restores the default priority of CAPWAP management packets.

The default priority of CAPWAP management packets is 7.

Format

capwap control-link-priority { **local** | **remote** } *priority-value*

undo capwap control-link-priority { **local** | **remote** }

Parameters

Parameter	Description	Value
local	Specifies the priority of CAPWAP management packets from the AC to the APs. The priority of CAPWAP management packets determines the reliability of links from the AC to APs.	-
remote	Priority of CAPWAP management packets from APs to the AC. The priority of CAPWAP management packets determines the reliability of links from APs to the AC.	-
priority-value	Specifies the priority of CAPWAP management packets.	The value is an integer that ranges from 0 to 7. The value 0 indicates the lowest priority, and the value 7 indicates the highest priority.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure the DSCP priority of CAPWAP management packets. A higher priority indicates a more reliable link between the AC and APs.

The configuration of the priority of CAPWAP management packets from the AC to APs takes effect immediately. After the priority of CAPWAP management packets from an AP to the AC is changed, if the AP is online, the AC sends the priority to the AP in the Echo packet. If the AP is not online, the priority is delivered to the AP in the Echo packet when the AP goes online. The new priority takes effect immediately when the AP receives it.

Precautions

NOTICE

When setting the parameter **local** *priority-value* to configure the priority of CAPWAP management packets from the AC to APs, ensure that the value is in the range of 4 to 7 to prevent the management channel from being interrupted in case of heavy service traffic.

Example

Set the priority of CAPWAP management packets from the AC to APs to 6.

```
<HUAWEI> system-view
[HUAWEI] capwap control-link-priority local 6
```

11.1.27 capwap dtls control-link encrypt

Function

The **capwap dtls control-link encrypt** command configures DTLS encryption for CAPWAP control tunnels.

The **undo capwap dtls control-link encrypt** command restores the default configuration of DTLS encryption for CAPWAP control tunnels.

By default, DTLS encryption for CAPWAP control tunnels is disabled.

Format

capwap dtls control-link encrypt

undo capwap dtls control-link encrypt

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the Discovery phase of the CAPWAP tunnel establishment between the AP and AC, the AP obtains the AC IP address using the discovery mechanism. Then in the DTLS negotiation phase, a CAPWAP tunnel is established between the AP and AC based on this IP address. During this process, UDP packets transmitted over the CAPWAP tunnel are encrypted using DTLS.

After DTLS encryption is enabled on the local end, the local end authenticates the peer end using the configured authentication mode. After authentication succeeds, the local end negotiates a DTLS encryption key with the peer end based on the authentication mode to protect packets transmitted over the CAPWAP control tunnel. If the DTLS negotiation fails, the CAPWAP tunnel cannot be established.

Configuration Impact

After the configuration is modified, the AP and AC re-establish a CAPWAP tunnel.

Precautions

Before enabling this function, run the **capwap dtls psk** command to configure a PSK.

If this function is enabled on the peer end, authentication and DTLS encryption negotiation are still performed on the local end even if the function is disabled on the local end. If the local end fails the verification of the peer end, the CAPWAP tunnel fails to be established. To temporarily disable DTLS encryption on the local and peer ends, you can configure the function of establishing CAPWAP DTLS sessions in none authentication mode. However, this function brings security risks. Ensure that the peer and local ends are in a secure and trusted network environment. After the CAPWAP link is established, disable the function of establishing CAPWAP DTLS sessions in none authentication mode so that the local and peer ends reestablish a CAPWAP link in secure mode.

Example

Enable DTLS encryption for CAPWAP control tunnels.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls control-link encrypt
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue? [Y/N]:y
```

11.1.28 capwap dtls cert-mandatory-match disable

Function

The **capwap dtls cert-mandatory-match disable** command disables the function of establishing CAPWAP DTLS sessions through the initial certificate.

The **undo capwap dtls cert-mandatory-match disable** command enables the function of establishing CAPWAP DTLS sessions through the initial certificate.

By default, the function of establishing CAPWAP DTLS sessions through the initial certificate is enabled.

Format

capwap dtls cert-mandatory-match disable

undo capwap dtls cert-mandatory-match disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If DTLS encryption for CAPWAP control tunnels has been enabled, when adding an AP running V200R021C00 or later, you can enable APs to establish DTLS sessions through the initial certificate so that they can properly go online. After the APs go online, they obtain new DTLS certificates to initiate DTLS sessions and go online again in secure mode. If high security is required, you can disable this function and use PSK authentication.

If an AP has been online on another WAC where the PSK for DTLS encryption is configured, the AP will fail to go online after being steered to the local WAC. In this case, you need to enable APs to establish DTLS sessions through the initial certificate so that they can properly go online. After the AP goes online, it obtains a new DTLS credential to establish a DTLS session and go online again in secure mode. Then, disable this function.

Example

Disable the function of establishing CAPWAP DTLS sessions through the initial certificate.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls cert-mandatory-match disable
```

11.1.29 capwap dtls no-auth enable

Function

The **capwap dtls no-auth enable** command enables the function of establishing CAPWAP DTLS sessions in none authentication mode.

The **undo capwap dtls no-auth enable** command disables the function of establishing CAPWAP DTLS sessions in none authentication mode.

By default, the function of establishing CAPWAP DTLS sessions in none authentication mode is disabled.

Format

capwap dtls no-auth enable

undo capwap dtls no-auth enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If DTLS encryption for CAPWAP control tunnels has been enabled, when adding an AP running a version earlier than V200R021C00, you can run this command to enable the AP to establish a DTLS session in none authentication mode so that the AP can properly go online. After the AP goes online, it obtains a new DTLS certificate to initiate a DTLS session in secure mode and go online again. To ensure network security, disable this function immediately after the AP goes online again to prevent unauthorized APs from accessing the network.

Example

Disable the function of establishing CAPWAP DTLS sessions in none authentication mode.

```
<HUAWEI> system-view
[HUAWEI] undo capwap dtls no-auth enable
```

11.1.30 capwap dtls psk

Function

The **capwap dtls psk** command configures a pre-shared key (PSK) used for DTLS encryption.

By default, no PSK used for DTLS encryption is configured.

Format

capwap dtls psk *psk-value*

Parameters

Parameter	Description	Value
psk-value	Specifies a PSK used for DTLS encryption.	The value is string of 48 or 68 characters in ciphertext (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'Ol*Gmt.V(%^%#**) or a string of 8 to 32 characters in plaintext (for example, **YsHsjx_202206**). The key must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters except the question mark (?) and space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During CAPWAP tunnel establishment, an AP establishes a DTLS session with an AC. If DTLS encryption has been enabled for CAPWAP control, sent management packets will be encrypted using DTLS. When the PSK is used for DTLS encryption, this command can be used to modify the PSK value in the DTLS session.

Follow-up Procedure

Run the **capwap dtls control-link encrypt** command to enable DTLS encryption for CAPWAP control tunnels.

Precautions

After the **capwap dtls psk** command configuration is complete, the new PSK will be automatically synchronized to the online APs that are working properly, but the

previous PSK still takes effect. The new PSK takes effect after these APs go online again.

Example

Set the PSK used for DTLS encryption to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls psk YsHsjx_202206
```

11.1.31 capwap echo

Function

The **capwap echo** command sets the CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections.

The **undo capwap echo** command restores the default CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections.

By default, the CAPWAP heartbeat detection interval is 25s and the number of CAPWAP heartbeat detections is 6.

If dual-link backup is enabled, the default number of CAPWAP heartbeat detections changes to 3.

Format

capwap echo { **interval** *interval-value* | **times** *times-value* } *

undo capwap echo { **interval** | **times** }

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the CAPWAP heartbeat detection interval, at which a detection packets are sent.	The value is an integer that ranges from 2 to 300, in seconds.
times *times-value*	Specifies the number of CAPWAP heartbeat detections. If no response is received after the specified number of times, the link is considered disconnected.	The value is an integer that ranges from 3 to 120.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined by CAPWAP, the AP and AC send handshake packets periodically to maintain the data channel and management channel between them. If the AP does not receive packets from the peer end within the specified number of heartbeat detection times, the AP considers that the link with the peer end is disconnected. The AP resets and releases the IP address. Then, the AP and AC reestablish a link. If the AC does not receive packets from the peer end within the specified number of heartbeat detection times, the AC disconnects the link and reports an error to the AP. After this command is executed, the AP and AC perform heartbeat detection based on the new configurations (including the detection interval and number of detections).

Precautions

If dual-link backup is enabled in a WDS scenario, the CAPWAP heartbeat detection interval is 25s and the number of CAPWAP heartbeat detections is 3. In this case, the WDS link is unstable and cannot ensure normal user access. You need to run this command to set the CAPWAP heartbeat detection interval to 25 seconds and the number of CAPWAP heartbeat detections to 6.

After the CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections are configured, the interval and the number of times for sending Echo packets are configured.

Radio traffic statistics packets are sent and received together with Echo packets.

If you set the CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections smaller than the default values, the CAPWAP link reliability is degraded. If the two parameters are set too high, APs can go online only after a heartbeat timeout. Exercise caution when you set the values. The default values are recommended.

Example

Set the CAPWAP heartbeat detection interval to 30s and the number of CAPWAP heartbeat detections to 3.

```
<HUAWEI> system-view
[HUAWEI] capwap echo interval 30 times 3
```

11.1.32 capwap dtls cbc

Function

The **capwap dtls cbc enable** command configures the CAPWAP DTLS server to establish DTLS sessions with DTLS clients running earlier versions using the CBC cipher suite.

The **capwap dtls cbc disable** command disables the CAPWAP DTLS server from using the CBC cipher suite to establish DTLS sessions with DTLS clients running earlier versions.

By default, CAPWAP DTLS compatibility with the CBC cipher suite is disabled.

Format

capwap dtls cbc enable

capwap dtls cbc disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In versions earlier than V200R021C00, CAPWAP clients support only the DTLS CBC cipher suite, which poses security risks. To establish CAPWAP DTLS sessions with these clients, run this command to enable compatibility with earlier versions.

Precautions

This function can be used only after the weak-encryption-algorithm plug-in is installed.

After this function is enabled, the TLS1_TXT_PSK_WITH_AES_256_CBC_SHA algorithm suite is used to set up DTLS sessions with CAPWAP DTLS clients running a version earlier than V200R021C00, which poses security risks.

After this function is disabled, CAPWAP links established based on earlier DTLS versions are disconnected, which may interrupt services.

Example

Enable CAPWAP DTLS compatibility with the CBC cipher suite.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls cbc enable
```

11.1.33 capwap dtls version1.0

Function

The **capwap dtls version1.0 enable** command configures the CAPWAP DTLS server to establish DTLS 1.0 sessions with DTLS clients running earlier versions.

The **capwap dtls version1.0 disable** command disables the CAPWAP DTLS server from establishing DTLS 1.0 sessions with DTLS clients running earlier versions.

By default, CAPWAP compatibility with DTLS 1.0 is disabled.

Format

capwap dtls version1.0 enable

capwap dtls version1.0 disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In versions earlier than V200R021C00, CAPWAP clients support only the DTLS 1.0 version, which poses security risks. To establish CAPWAP DTLS sessions with clients that support only DTLS 1.0, run this command to enable compatibility with earlier versions.

Precautions

This function can be used only after the weak-encryption-algorithm plug-in is installed.

After this function is enabled, the DTLS 1.0 version is used to set up DTLS sessions with CAPWAP DTLS clients running a version earlier than V200R021C00, which poses security risks.

After this function is disabled, CAPWAP links established based on earlier DTLS versions are disconnected, which may interrupt services.

Example

Enable CAPWAP compatibility with DTLS 1.0.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls version1.0 enable
```

11.1.34 capwap echo-timeout trace logging

Function

The **capwap echo-timeout trace logging** command enables the Echo packet process trace and diagnostic log record functions upon AP Echo packet timeout.

The **undo capwap echo-timeout trace logging** command disables the Echo packet process trace and diagnostic log record functions upon AP Echo packet timeout.

By default, the Echo packet process trace and diagnostic log record functions are enabled upon AP Echo packet timeout.

Format

capwap echo-timeout trace logging

undo capwap echo-timeout trace logging

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you run the **capwap echo-timeout trace logging** command, the Echo packet process is traced and diagnostic logs are recorded upon AP Echo packet timeout.

Example

s

Enable the Echo packet process trace and diagnostic log record functions upon AP Echo packet timeout.

```
<HUAWEI> system-view
[HUAWEI] capwap echo-timeout trace logging
```

11.1.35 capwap message-integrity psk

Function

The **capwap message-integrity psk** command configures a PSK used for checking integrity of CAPWAP packets.

The **undo capwap message-integrity psk** command restores the default PSK used for checking integrity of CAPWAP packets.

The default username and password are available in *WLAN 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

capwap message-integrity psk *psk-value*

undo capwap message-integrity psk

Parameters

Parameter	Description	Value
psk-value	Specifies the PSK used for checking integrity of CAPWAP packets.	The value is string of 48 or 68 characters in ciphertext (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'Ol*Gmt.V(%^%#**) or a string of 6 to 32 characters in plaintext (for example, **YsHsjx_202206**). The key must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters except the question mark (?) and space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CAPWAP packets are transmitted between the AC and APs. To prevent the packets from being forged or tampered with and prevent malformed packet attacks, you can configure integrity check of CAPWAP packets. When a PSK is used to check integrity of CAPWAP packets, you can run this command on the AC to configure a PSK.

NOTE

It is recommended that you change the PSK in a timely manner to ensure device security.

Follow-up Procedure

Run the **undo capwap message-integrity check disable** command to enable integrity check of CAPWAP packets.

Configuration Impact

After the configuration is complete, all online APs on the AC go offline.

Example

Set the PSK used for checking integrity of CAPWAP packets to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] capwap message-integrity psk YsHsjx_202206
Warning: In a backup scenario, the PSK and status of CAPWAP message integrity check must be the same between the master and backup e
nds. This operation may cause devices using CAPWAP connections to reset or go offline. Continue? [Y/N]:y
```

11.1.36 capwap message-integrity check disable

Function

The **capwap message-integrity check disable** command disables integrity check of CAPWAP packets.

The **undo capwap message-integrity check disable** command enables integrity check of CAPWAP packets.

By default, integrity check of CAPWAP packets is enabled.

Format

capwap message-integrity check disable

undo capwap message-integrity check disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CAPWAP packets are transmitted between the AC and APs. To prevent the packets from being forged or tampered with and prevent malformed packet attacks, you can configure integrity check of CAPWAP packets.

Configuration Impact

After the configuration is modified, all online APs on the AC go offline.

Example

Enable integrity check of CAPWAP packets.

```
<HUAWEI> system-view
[HUAWEI] capwap message-integrity check disable
Warning: In a backup scenario, the PSK and status of CAPWAP message integrity check must be the same between the master and backup e
nds. This operation may cause devices using CAPWAP connections to reset or go offline. Continue? [Y/N]:y
```

11.1.37 capwap sensitive-info psk

Function

The **capwap sensitive-info psk** command configures a PSK used for encrypting sensitive information.

The **undo capwap sensitive-info psk** command restores the default PSK used for encrypting sensitive information.

The default username and password are available in *WLAN 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

capwap sensitive-info psk *psk-value*

undo capwap sensitive-info psk

Parameters

Parameter	Description	Value
psk-value	Specifies the PSK used for encrypting sensitive information.	The value is string of 48 or 68 characters in ciphertext (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'Ol*Gmt.V(%^%#**) or a string of 6 to 32 characters in plaintext (for example, **YsHsjx_202206**). The key must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters except the question mark (?) and space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Sensitive information exchanged between the AC and APs is encrypted, such as the FTP user name/password, AP login user name/password, and service configuration-related keys. You can run this command to modify the PSK used for encrypting sensitive information.

NOTE

It is recommended that you change the PSK in a timely manner to ensure device security.

After the configuration is complete, all online APs on the AC go offline and online again.

Precautions

In dual-link HSB and cold backup scenarios, ensure that the PSKs configured on the active and standby ACs are the same. Otherwise, APs cannot establish

CAPWAP tunnels with the standby ACs, causing the APs to go offline after an active/standby switchover.

When an AP is being upgraded on the AC, the PSK used for encrypting sensitive information cannot be changed.

Example

Set the PSK for encrypting sensitive information to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] capwap sensitive-info psk YsHsjx_202206
Warning: This operation may cause devices using CAPWAP connections to go offline. Continue? [Y/N]:y
```

11.1.38 capwap source interface

Function

The **capwap source interface** command configures the interface used by the AC to establish a CAPWAP tunnel as the source interface of the AC.

The **undo capwap source interface** command disables the AC from using an interface as the source interface.

By default, no source interface is configured for the AC.

Format

capwap source interface { **loopback** *loopback-number* | **vlanif** *vlan-id* }

undo capwap source interface { **loopback** *loopback-number* | **vlanif** *vlan-id* }

Parameters

Parameter	Description	Value
loopback *loopback-number*	Configures a loopback interface as the source interface.	The value is an integer that ranges from 0 to 1023.
vlanif *vlan-id*	Configures a VLANIF interface as the source interface.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source IP address must be specified for each AC so that all access devices connected to the AC can learn this IP address for communication.

When the CAPWAP source interface or address is configured for the first time, the system checks whether security-related configurations exist, including the PSK for DTLS encryption, PSK for DTLS encryption of inter-AC tunnels, user name and password for logging in to the AP, and password for logging in to the global offline management VAP. The CAPWAP source interface or address can be successfully configured only when all these configurations exist; otherwise, the system prompts you to complete related configurations first.

Prerequisites

An IP address has been assigned to the specified loopback or VLANIF interface.

Precautions

A maximum of eight source interfaces can be configured.

If SVF is enabled, only one source interface can be configured.

When multiple source interfaces are configured, the management VLAN of the APs must be within the VLAN range corresponding to the source interfaces. Otherwise, the APs cannot go online.

The source interface cannot be bound to a VPN instance.

Changing the source interface configuration will clear statistics about CAPWAP packets in CPU attack defense.

Example

Configure a loopback interface as the source interface.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 20
[HUAWEI-LoopBack20] ip address 192.168.10.1 24
[HUAWEI-LoopBack20] quit
[HUAWEI] capwap source interface loopback 20
Set the DTLS PSK(contains 6-32 plain-text characters, or 48 or 68 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):******

Set the DTLS inter-controller PSK(contains 6-32 plain-text characters, or 48 or 68 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):******

Set the user name for FIT APs(contains 4-31 plain-text characters, which can only include letters, digits and underlines. And the first character must be a letter):admin

Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188 characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):********

Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):********
```


Table 11-1 Description of the command output

Item	Description
Set the DTLS PSK	Configures the PSK for DTLS encryption.
Set the DTLS inter-controller PSK	Configures the PSK for DTLS encryption of inter-AC tunnels.
Set the user name for FIT APs Set the password for FIT APs	Configures the user name and password for logging in to the Fit AP.
Set the global temporary-management psk	Configures the password for logging in to the global offline management VAP, allowing users to connect to the offline management SSID in wireless mode.

11.1.39 channel

Function

(AP group radio view) The **channel** command configures the working bandwidth and channel for specified radios on all APs in an AP group.

(AP group radio view) The **undo channel** command restores the default working bandwidth and channel for specified radios on all APs in an AP group.

(AP radio view) The **channel** command configures the working bandwidth and channel for specified radios on an AP.

(AP radio view) The **undo channel** command restores the working bandwidth and channel on specified radios of an AP to those configured in the AP group radio view.

By default, the working bandwidth of a radio is 20 MHz, and no working channel is configured for a radio.

Format

channel { **20mhz** | **40mhz-minus** | **40mhz-plus** | **80mhz** | **160mhz** | **320mhz** } *channel*

channel 80+80mhz *channel1 channel2*

undo channel

Parameters

Parameter	Description	Value
20mhz	Sets the working bandwidth of a radio to 20 MHz.	-
40mhz-minus	Sets the working bandwidth of a radio to 40 MHz Minus.	-
40mhz-plus	Sets the working bandwidth of a radio to 40 MHz Plus.	-
80mhz	Sets the working bandwidth of a radio to 80 MHz.	-
160mhz	Sets the working bandwidth of a radio to 160 MHz.	-
320mhz	Sets the working bandwidth of a radio to 320 MHz.	-
80+80mhz	Sets the working bandwidth of a radio to 80+80 MHz.	-
channel/ channel1/ channel2	Specifies the working channel of a radio.	The parameter is an enumeration value. The value range is determined based on the country code and radio mode.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different radios use different channels. Channels for radios also vary in different countries and regions. Select channels based on the actual situations.

Precautions

The channel parameter settings must match the radio frequency band. For details about mappings between channel parameters and frequency bands, see *Country Codes & Channels Compliance*. You can obtain this table at Huawei technical support website.

- Enterprise technical support website: **https://support.huawei.com/enterprise**

- Carrier technical support website: **https://support.huawei.com**

The configured channels must be supported by STAs; otherwise, the STAs cannot discover radio signals.

If an AP detects radar signals on a channel, the channel cannot be configured as the radio channel of the AP in 30 minutes. However, the channel can be configured as the radio channel of other APs that do not detect radar signals on it.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

If two radios of an AP work on the 5 GHz frequency band, the operating channels of the two 5 GHz radios must be separated by at least one channel to avoid interference. If two radios of an AP work on the 5 GHz and 6 GHz frequency bands, respectively, pay attention to channel planning as follows:

- For the model AirEngine 6761-22T: Do not use a 5 GHz high-frequency channel (149–165) and a 6 GHz low-frequency channel (80 MHz channels 1–13, 160 MHz channels 1–29) at the same time.
- For the model AirEngine 8771-X1T: Do not use a 5 GHz high-frequency channel (20 MHz channels 153–165, 40 MHz channels 132–161, 80 MHz channels 132–161, 160 MHz channels 100–128, 320 MHz channels 100–144) and a 6 GHz channel (160 MHz channels 1–29, 320 MHz channels 1–61) at the same time.

For example, a country supports 40 MHz+ 5G channels 36, 44, 52, and 60. When deploying 5 GHz radio channels, if one radio is deployed to work on channel 36, it is recommended that channel 52 or 60 be configured for the other radio. Channel 44 is not recommended in this case.

NOTE

- You can configure the 80 MHz, 160 MHz, 320 MHz, or 80+80 MHz bandwidth only in the 5G radio view. When 320 MHz bandwidth is configured on the 5 GHz frequency band, the available channels are fixed at 100–144 that operate with 240 MHz bandwidth.

Example

Set the working bandwidth to 20 MHz and channel to 6 for radio 0 of AP 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.40 channel-switch announcement disable

Function

The **channel-switch announcement disable** command disables an AP from sending an announcement when the channel is switched.

The **undo channel-switch announcement disable** command enables an AP to send an announcement when the channel is switched.

By default, an AP sends an announcement when the channel is switched.

Format

channel-switch announcement disable

undo channel-switch announcement disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

When the AP works on a Depth First Select (DFS) channel, a radar detection is performed. The AP automatically switches to another channel because the DFS channel frequency may interfere with the radar frequency.

After the **undo channel-switch announcement disable** command is run, if the AP channel switches, the AP sends an Action frame to instruct STAs to switch channels after multiple Beacon intervals. The AP also switches the channel after the same intervals. The AP and STAs switch channels at the same time to prevent STA reassociations and ensure rapid service recovery.

NOTE

The channel switching announcement function must be supported by both the AP and STA.

The following APs do not send Action frames during channel switching announcement. Instead, these APs carry information in Beacon frames to instruct STAs to switch channels.

- AirEngine 9700D-S (including matching ORUs)
- AirEngine X77X
- AirEngine X76X

Example

Disable the AP from sending an announcement after the channel is switched.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] channel-switch announcement disable
```

11.1.41 channel-switch mode

Function

The **channel-switch mode** command configures an announcement mode for channel switching.

The **undo channel-switch mode** command restores the default announcement mode for channel switching.

By default, data transmission from STAs continues on the current channel when the channel is switched.

Format

channel-switch mode { **stop-transmitting** | **continue-transmitting** }

undo channel-switch mode

Parameters

Parameter	Description	Value
stop-transmitting	Stops data transmission from STAs on the current channel during channel switching.	-
continue-transmitting	Continues data transmission from STAs on the current channel during channel switching.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

During channel switching, STA communication is interrupted. The administrator can stop an associated STA sending data on the current channel until channel switching is complete. Alternatively, data transmission from STAs can be continued on the current channel before channel switching is complete.

Example

Stop data transmission from STAs on the current channel during channel switching.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] channel-switch mode stop-transmitting
```


11.1.42 copy-from

Function

The **copy-from** command copies data to the current profile from a profile of the same type.

Format

copy-from *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the profile from which data is copied.	The profile name must already exist.

Views

All WLAN profile views except the WIDS profile, WIDS whitelist profile, and WIDS spoof SSID profile

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **copy-from** command to copy data to the current profile from a profile of the same type. This simplifies profile configuration and improves configuration efficiency.

- To create a profile that has the same configuration as an existing profile, enter the view of the profile to be created and run the **copy-from** command to copy data from the existing profile.
- To create a profile that has most configurations the same as an existing profile, enter the view of the new profile, run the **copy-from** command to copy data from the existing profile, and modify the different configurations.

Precautions

If the current profile is referenced by another profile, you cannot run the command to copy data to the current profile.

When the WAPI certificate or private key configuration exists in the security profile, you must manually perform the configuration instead of using this command to copy data.

When you copy a location profile, if the protocol used by APs to report information is set to HTTPS and the SSL policy (**private report-protocol https ssl-policy** *ssl-policy*) is specified, the configuration will not be copied.

Example

Create the VAP profile **test** and copy data from the profile **sample**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-wlan-vap-prof-test] copy-from sample
```

11.1.43 country-code

Function

The **country-code** command configures a country code.

The **undo country-code** command restores the default country code.

The default country code is **CN**.

Format

country-code *country-code*

undo country-code

Parameters

Parameter	Description	Value
country-code	Specifies a country code.	The value is a string of characters in enumerated type. For specific values, see **Table 11-2**.

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Table 11-2 Country codes supported by ACs

Country Code	Country/Region
AE	United Arab Emirates
AM	Armenia
AR	Argentina
AT	Austria
AU	Australia
AZ	Azerbaijan
BE	Belgium
BG	Bulgaria
BH	Bahrain
BN	Brunei Darussalam
BO	Bolivia
BR	Brazil
BY	Belarus
BZ	Belize
CA	Canada
CH	Switzerland
CL	Chile
CN	China (default)
CO	Colombia
CR	Costa Rica
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
EC	Ecuador
EE	Estonia
EG	Egypt

Country Code	Country/Region
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GE	Georgia
GR	Greece
GT	Guatemala
HK	Hong Kong, China
HN	Honduras
HR	Croatia
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India
IQ	Iraq
IR	Iran
IS	Iceland
IT	Italy
JO	Jordan
JP	Japan
KE	Kenya
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania

Country Code	Country/Region
LU	Luxembourg
LV	Latvia
MA	Morocco
MC	Monaco
MK	Republic of North Macedonia
MO	Macao, China
MT	Malta
MX	Mexico
MY	Malaysia
NG	Nigeria
NL	Netherlands
NO	Norway
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PH	Philippines
PK	Pakistan
PL	Poland
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RS	Serbia
RU	Russia
SA	Saudi Arabia
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia

Country Code	Country/Region
SV	El Salvador
SY	Syria
TH	Thailand
TN	Tunisia
TR	Türkiye
TT	Trinidad and Tobago
TW	Taiwan, China
UA	Ukraine
US	United States
UY	Uruguay
UZ	Uzbekistan
VE	Venezuela
VN	Vietnam
YE	Yemen
ZA	South Africa
ZW	Zimbabwe

Usage Scenario

When an AC controls APs in different countries or regions, different country codes can be configured based on the regulatory domain profile to meet different radio requirements, such as power and channel specifications, in different countries or regions.

Configuration Impact

After the country code is changed in a regulatory domain profile, APs using the regulatory domain profile automatically restart if they run versions earlier than V200R020C00.

Example

Set the country code to **US** in the regulatory domain profile **region1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name region1
[HUAWEI-wlan-regulate-domain-region1] country-code us
Warning: Modifying the country code will clear the channel and power configurations of radios, and
requires the APs to be restarted if they run V200R019C10 or earlier. Continue?[Y/N]:y
```


11.1.44 coverage distance

Function

(AP group radio view) The **coverage distance** command configures the radio coverage distance parameter for all specified radios in an AP group.

(AP group radio view) The **undo coverage distance** command restores the default radio coverage distance parameter for all specified radios in an AP group.

(AP radio view) The **coverage distance** command configures the radio coverage distance parameter for an AP radio.

(AP radio view) The **undo coverage distance** command restores the configuration of the radio coverage distance parameter on an AP radio to that configured in the AP group radio view.

By default, the radio coverage distance parameter is 3 (unit: 100 m) for all radios.

Format

coverage distance *distance*

undo coverage distance

Parameters

Parameter	Description	Value
distance	Specifies the radio coverage distance parameter. Each distance parameter corresponds to a group of **slottime**, **acktimeout**, and **ctstimeout** values. You can configure the radio coverage distance based on the AP distance, so that APs adjust the **slottime**, **acktimeout**, and **ctstimeout** values accordingly.	The value is an integer that ranges from 1 to 400, in the unit of 100 meters.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, two APs may be deployed at a spacing of dozens of meters to dozens of kilometers. Therefore, the time to wait for ACK frames from the peer AP varies

depending on the AP spacing. A proper ACK timeout setting can improve data transmission efficiency between APs.

You can configure the radio coverage distance parameter based on distances between APs. Based on this parameter, the APs can automatically adjust the values of **slottime**, **acktimeout**, and **ctstimeout** to improve data transmission efficiency.

Precautions

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Example

Set the radio coverage distance parameter to 2 for radio 0 of AP 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] coverage distance 2
```

11.1.45 cpe-tunnel-profile (WLAN view)

Function

The **cpe-tunnel-profile** command creates a CPE tunnel profile and displays the CPE tunnel profile view, or displays the view of an existing CPE tunnel profile.

The **undo cpe-tunnel-profile** command deletes a CPE tunnel profile.

No default CPE tunnel profile is available in the system.

Format

cpe-tunnel-profile name *profile-name*

undo cpe-tunnel-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a CPE tunnel profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all CPE tunnel profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An EoGRE tunnel established between an AP and a CPE is also known as a CPE tunnel. A CPE tunnel profile is used to specify the parameters including the VLAN, GRE key, and GRE checksum used by the CPE tunnel.

Follow-up Procedure

Run the **cpe-tunnel-profile** command in the VAP profile view to bind the CPE tunnel profile to a VAP profile and run the **vap-profile** command to bind the VAP profile to an AP group, AP, AP radio, or AP group radio so that the CPE tunnel profile can take effect.

Precautions

- A CPE tunnel profile bound to a VAP profile cannot be deleted. To delete such a CPE tunnel profile, unbind it from the VAP profile first.

Example

Create the CPE tunnel profile **cpe1** and display the CPE tunnel profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] cpe-tunnel-profile name cpe1
[HUAWEI-wlan-cpe-tunnel-prof-cpe1]
```

11.1.46 cpe-tunnel-profile (VAP profile view)

Function

The **cpe-tunnel-profile** command binds a CPE tunnel profile to a VAP profile.

The **undo cpe-tunnel-profile** command unbinds a CPE tunnel profile from a VAP profile.

By default, no CPE tunnel profile is bound to a VAP profile.

Format

cpe-tunnel-profile *profile-name*

undo cpe-tunnel-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a CPE tunnel profile.	The CPE tunnel profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

The EoGRE tunnel encapsulation function has been enabled on a CPE.

Usage Scenario

After a CPE tunnel profile is bound to a VAP profile, data packets of wired terminals connected to a CPE are transparently transmitted to the upper-layer wired network through the CPE tunnel.

Example

Create the CPE tunnel profile **cpe1** and bind it to the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] cpe-tunnel-profile name cpe1
[HUAWEI-wlan-cpe-tunnel-prof-cpe1] quit
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] cpe-tunnel-profile cpe1
```

11.1.47 deny-broadcast-probe enable

Function

The **deny-broadcast-probe enable** command configures an AP not to respond to broadcast Probe Request frames.

The **undo deny-broadcast-probe enable** command configures an AP to respond to broadcast Probe Request frames.

By default, an AP responds to broadcast Probe Request frames.

Format

deny-broadcast-probe enable

undo deny-broadcast-probe enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many Probe Response frames occupy a large number of wireless resources. To reduce wireless resource occupation of the frames and improve channel usage efficiency, you can run the **deny-broadcast-probe enable** command to configure an AP not to respond to broadcast Probe Request frames.

Precautions

Configuring an AP not to respond to broadcast Probe Request frames may reduce channel scan efficiency of some STAs.

Example

Configure an AP not to respond to broadcast Probe Request frames.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] deny-broadcast-probe enable
```

11.1.48 destination (soft GRE profile view)

Function

The **destination** command configures the destination IP address for a soft GRE tunnel.

The **undo destination** command restores the default destination IP address of a soft GRE tunnel.

By default, no destination IP address is configured for a soft GRE tunnel.

Format

destination { **ip-address** *destination-ip-address* | **ipv6-address** *destination-ipv6-address* }

undo destination

Parameters

Parameter	Description	Value
ip-address *destination-ip-address*	Specifies the destination IPv4 address of a soft GRE tunnel.	The value is in dotted decimal notation.
ipv6-address *destination-ipv6-address*	Specifies the destination IPv6 address of a soft GRE tunnel.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

Soft GRE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the soft GRE forwarding mode, you need to configure the destination IP address of the soft GRE tunnel, that is, the peer IP address of the tunnel, so that service data can be forwarded to the specified destination IP address.

Precautions

Ensure that the route between the AP and the destination IP address of the soft GRE tunnel is reachable.

The destination IP address of a soft GRE tunnel must be configured in a soft GRE profile. The destination IP addresses of different soft GRE profiles cannot be the same.

If the IP address type of the AP is different from the destination IP address type configured in the soft GRE profile, the AP cannot establish a soft GRE tunnel.

If this command is run more than once, the latest configuration overrides the previous one.

Example

Set the destination IP address of a soft GRE tunnel to 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] softgre-profile name soft1
[HUAWEI-wlan-softgre-prof-soft1] destination ip-address 10.10.1.1
```


11.1.49 dhcp client option12

Function

The **dhcp client option12** command enables or disables DHCP packets sent by APs to carry the Option 12 field and specifies AP information contained in the Option 12 field.

The **undo dhcp client option12** command restores the default AP information in the Option 12 field carried in DHCP packets sent by APs.

By default, the Option 12 field carried in DHCP packets sent by an AP contains the AP type and MAC address.

Format

dhcp client option12 { **ap-name** | **ap-type ap-mac** | **disable** }

undo dhcp client option12

Parameters

Parameter	Description	Value
ap-name	Enables DHCP packets sent by APs to carry the Option 12 field that contains the AP name.	-
ap-type ap-mac	Enables DHCP packets sent by APs to carry the Option 12 field that contains the AP type and MAC address.	-
disable	Disables DHCP packets sent by APs from carrying the Option 12 field.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP (DHCP client) obtains an IP address through DHCP, this function enables the DHCP Discover and DHCP Request packets sent by the AP to carry the Option 12 field. The Option 12 field can contain the AP type, MAC address or the AP name. After the AP obtains an IP address through DHCP, you can check information about the AP with this IP address on the DHCP server that supports display of DHCP client host information.

Precautions

This function is valid only for the APs that obtain IP addresses through DHCP.

Example

Configure the AP name contained in the Option 12 field carried in DHCP packets sent by APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] dhcp client option12 ap-name
```

11.1.50 dhcp option82 insert enable

Function

The **dhcp option82 insert enable** command enables the function of adding the Option 82 field to DHCP packets sent by STAs.

The **undo dhcp option82 insert enable** command disables the function of adding the Option 82 field to DHCP packets sent by STAs.

By default, the function of adding the Option 82 field to DHCP packets sent by STAs is disabled.

Format

dhcp option82 insert enable

undo dhcp option82 insert enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After going online, a STA obtains the IP address through DHCP. When the DHCP Request packet from the STA reaches an AP, the AP adds the Option 82 field to the packet and sends the packet to the DHCP server. The Option 82 field contains the MAC address or SSID of the associated AP. Therefore, the DHCP server knows the AP on which the STA goes online.

Prerequisites

Before enabling the function of adding the Option 82 field to DHCP packets sent by STAs, run the **undo learn-client-address disable** command to enable the STA IP address learning. By default, STA IP address learning is enabled.

Example

Enable the function of adding the Option 82 field to DHCP packets sent by STAs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] dhcp option82 insert enable
```

11.1.51 dhcp option82 format (VAP profile view)

Function

The **dhcp option82 format** command configures the format of the Option 82 field in DHCP messages sent from STAs.

The **undo dhcp option82 format** command restores the default format of the Option 82 field in DHCP messages sent from STAs.

By default, the format of the Option 82 field in DHCP messages sent from STAs is **ap-mac**.

Format

dhcp option82 { **circuit-id** | **remote-id** } **format** { **ap-mac** [**mac-format** { **normal** | **compact** | **hex** | **colon** }] [**user-defined** *text*] | **ap-mac-ssid** [**mac-format** { **normal** | **compact** | **colon** }] [**user-defined** *text*] | **user-defined** *text* | **ap-name** [**user-defined** *text*] | **ap-name-ssid** [**user-defined** *text*] | **ap-location** [**user-defined** *text*] | **ap-location-ssid** [**user-defined** *text*] }

dhcp option82 { **remote-id** | **circuit-id** } **format** { **ap-group-ap-mac** | **ap-group-ap-mac-ssid** } **mac-format** { **normal** | **compact** | **colon** } [**user-defined** *text*]

dhcp option82 { **remote-id** | **circuit-id** } **format** { **ap-group** | **ap-group-ap-name** | **ap-group-ap-name-ssid** | **ap-group-ap-location** | **ap-group-ap-location-ssid** } [**user-defined** *text*]

undo dhcp option82 { **circuit-id** | **remote-id** } **format**

Parameters

Parameter	Description	Value
circuit-id	Specifies the circuit-ID in the Option 82 field.	-
remote-id	Specifies the remote-ID in the Option 82 field.	-

Parameter	Description	Value
ap-mac	Indicates that Option 82 contains the AP's MAC address.	-
ap-mac-ssid	Indicates that Option 82 contains the AP's MAC address and SSID.	-
mac-format	Specifies the format of the AP's MAC address in Option 82.	-
normal	Sets the MAC address format to xx-xx-xx-xx-xx-xx.	-
compact	Sets the MAC address format to xxxx-xxxx-xxxx.	-
hex	Sets the MAC address format to XXXXXXXXXXXX in hexadecimal notation.	-
colon	Sets the MAC address format to xx:xx:xx:xx:xx:xx.	-
user-defined *text*	Specifies the user-defined format of Option 82.	The value is a string of 1 to 255 characters.
ap-name	Indicates that Option 82 contains the AP name.	-
ap-name-ssid	Indicates that Option 82 contains the AP name and SSID.	-
ap-location	Indicates that Option 82 contains the AP location.	-
ap-location-ssid	Indicates that Option 82 contains the AP location and SSID.	-
ap-group	Indicates that Option 82 contains the AP group name.	-
ap-group-ap-mac	Indicates that Option 82 contains the AP group name and AP's MAC address.	-
ap-group-ap-mac-ssid	Indicates that Option 82 contains the AP group name, AP's MAC address, and SSID.	-

Parameter	Description	Value
ap-group-ap-name	Indicates that Option 82 contains the AP group name and AP name.	-
ap-group-ap-name-ssid	Indicates that Option 82 contains the AP group name, AP name, and SSID.	-
ap-group-ap-location	Indicates that Option 82 contains the AP group name and AP location.	-
ap-group-ap-location-ssid	Indicates that Option 82 contains the AP group name, AP location, and SSID.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

After the function of adding the Option 82 field to DHCP messages sent from STAs, you can run the **dhcp option82 format** command to configure the format of the Option 82 field.

You can use the following keywords to define the Option 82 field:

- ap-mac: indicates the AP's MAC address. After DHCP messages from a STA reach an AP, the AP inserts its MAC address into the Option 82 field of the DHCP messages.
- ap-mac-ssid: indicates the MAC address and SSID of the AP. After DHCP messages from a STA reach an AP, the AP inserts its MAC address and SSID associated with the STA into the Option 82 field of the DHCP messages.
- ap-name: indicates the AP name. After DHCP messages from a STA reach an AP, the AP inserts its name into the Option 82 field of the DHCP messages.
- ap-name-ssid: indicates the AP name and SSID. After DHCP messages from a STA reach an AP, the AP inserts its name and associated SSID into the Option 82 field of the DHCP messages.
- ap-location: indicates the AP location. After DHCP messages from a STA reach an AP, the AP inserts its location into the Option 82 field of the DHCP messages.
- ap-location-ssid: indicates the AP location and SSID. After DHCP messages from a STA reach an AP, the AP inserts its location and associated SSID into the Option 82 field of the DHCP messages.
- ap-group: indicates the AP group name. After DHCP messages from a STA reach an AP, the AP inserts the name of the AP group to which it belongs into the Option 82 field of the DHCP messages.

- ap-group-ap-mac, ap-group-ap-mac-ssid, ap-group-ap-name, ap-group-ap-name-ssid, ap-group-ap-location, ap-group-ap-location-ssid: indicates the combination of the AP group name and other keywords. After DHCP messages from a STA reach an AP, the AP inserts the name of the AP group to which it belongs and information specified by other keywords into the Option 82 field of the DHCP messages.

If **mac-format** is not specified in the **dhcp option82** { **circuit-id** | **remote-id** } **format** { **ap-mac** | **ap-mac-ssid** } command, the AP's MAC address in the Option 82 field is **XXXXXXXXXXXX** in ASCII format.

The total length of the **circuit-id** and **remote-id** options in the Option 82 field cannot exceed 255 bytes. Otherwise, some Option 82 information may be lost. Note that a Chinese character may occupy 2 or 3 bytes.

Example

Set the format of the remote-ID suboption in Option 82 carried in DHCP messages sent from STAs to **ap-mac-ssid**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] dhcp option82 remote-id format ap-mac-ssid
```

11.1.52 display ac global configuration

Function

The **display ac global configuration** command displays AC global configuration.

Format

display ac global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view AC global information.

Example

Display AC global configuration.


```
<HUAWEI> display ac global configuration
------------------------------------------------------------------------------
AC sysnetid                    : AC
------------------------------------------------------------------------------
```

Table 11-3 Description of the **display ac global configuration** command output

Item	Description
AC sysnetid	NE name of an AC. To configure the NE name for an AC, run the **ac sysnetid** command.

11.1.53 display ap

Function

The **display ap** command displays AP information.

Format

display ap { **all** | **ap-group** *ap-group* }

display ap [**ap-group** *ap-group*] **by-ssid** *ssid*

display ap by-state *state* [**ap-group** *ap-group*]

Parameters

Parameter	Description	Value
all	Displays information about all APs.	-
ap-group *ap-group*	Specifies the AP group to which an AP belongs.	The AP group must exist.
by-ssid *ssid*	Specifies an SSID.	The SSID must exist.

Parameter	Description	Value
by-state *state*	Displays the status of an AP.	The value is of the enumerated type: • **commit-failed**: Displays information about APs in configuration commitment failed state. • **committing**: Displays information about APs in configuration committing state. • **config**: Displays information about APs in configuration initialization state. • **config-failed**: Displays information about APs in initialization failed state. • **download**: Displays information about APs in system software downloading state. • **fault**: Displays information about APs that failed to go online. • **idle**: Displays information about APs in initialization state before the link is established for the first time.

Parameter	Description	Value
		• **name-conflicted**: Displays information about APs having duplicate names. • **normal**: Displays information about APs in normal state. • **standby**: Displays information about APs in standby state. • **ver-mismatch**: Displays information about APs with versions that do not match the AC version. • **countrycode-mismatch**: Displays information about APs with country codes that do not match the AC's country code. • **type-mismatch**: Displays information about APs with types that are different from the actual types.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about APs, run this command.

Example

Display information about all APs.

```
<HUAWEI> display ap all
Total AP information:
nor  : normal          [2]
ExtraInfo : Extra information
P    : insufficient power supply
D    : data link exception
--------------------------------------------------------------------------------------------------
ID   MAC           Name   Group     IP             Type               State STA Uptime      ExtraInfo Scene
--------------------------------------------------------------------------------------------------
0    00e0-fcf6-76a0 area_1 ap-group1 192.168.120.254 AirEngine8760-X1-PRO   nor   0   4H:49M:11S
P         -
1    00e0-fc74-9640 area_2 ap-group1 192.168.120.253 AirEngine8760-X1-PRO   nor   0   6H:3M:40S
-         -
--------------------------------------------------------------------------------------------------
Total: 2
```

Display information about APs bound to the SSID **guest-wlan**.

```
<HUAWEI> display ap by-ssid guest-wlan
Total AP information:
nor  : normal          [2]
ExtraInfo : Extra information
P  : insufficient power supply
D    : data link exception
--------------------------------------------------------------------------------------------------
ID   MAC           Name   Group     IP             Type               State STA Uptime      ExtraInfo Scene
--------------------------------------------------------------------------------------------------
0    00e0-fcf6-76a0 area_1 ap-group1 192.168.120.254 AirEngine8760-X1-PRO   nor   0   4H:49M:11S
P         -
1    00e0-fc74-9640 area_2 ap-group1 192.168.120.253 AirEngine8760-X1-PRO   nor   0   6H:3M:40S
-         -
--------------------------------------------------------------------------------------------------
Total: 2
```

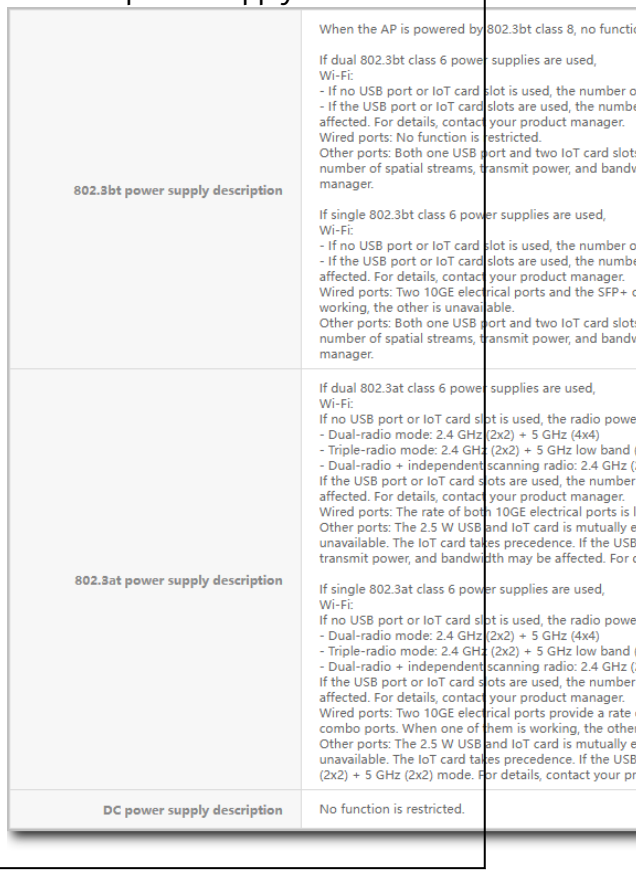
Display information about APs in normal state.

```
<HUAWEI> display ap by-state normal
Total AP information:
nor  : normal          [2]
ExtraInfo : Extra information
P  : insufficient power supply
D    : data link exception
--------------------------------------------------------------------------------------------------
ID   MAC           Name   Group     IP             Type               State STA Uptime      ExtraInfo Scene
--------------------------------------------------------------------------------------------------
0    00e0-fcf6-76a0 area_1 ap-group1 192.168.120.254 AirEngine8760-X1-PRO   nor   0   4H:49M:11S
P         -
1    00e0-fc74-9640 area_2 ap-group1 192.168.120.253 AirEngine8760-X1-PRO   nor   0   6H:3M:40S
-         -
--------------------------------------------------------------------------------------------------
Total: 2
```

Table 11-4 Description of the **display ap** command output

Item	Description
ID	AP ID.
MAC	MAC address of an AP.

Item	Description
Name	AP name.
Group	Name of the AP group to which an AP belongs.
IP	IP address of an AP.
Type	AP type.
State	AP state. For details, see **Table 11-5**.
STA	Number of STAs connected to an AP.
Uptime	Online duration of an AP.

Item	Description
ExtraInfo	Extra information. • -: indicates that no extra information is configured. • **P: insufficient power supply**: indicates that the AP is working in Limited or Insufficient state due to insufficient power supply and some functions are limited or unavailable. For the specific mode, you can run the **display ap power-workmode** command to check the value of the **Power-workmode** field. When the power supply is insufficient, the impact on the AP functions and performance varies depending on AP models. For Huawei AirEngine series APs: Check the power supply downgrade limit as follows: Visit **Info-Finder**, select a product series, and view hardware specifications in the hardware center. You can check the power supply downgrade limits at different power supply levels.  802.3bt power supply description When the AP is powered by 802.3bt class 8, no functio If dual 802.3bt class 6 power supplies are used, Wi-Fi: - If no USB port or IoT card slot is used, the number o - If the USB port or IoT card slots are used, the numbe affected. For details, contact your product manager. Wired ports: No function is restricted. Other ports: Both one USB port and two IoT card slots number of spatial streams, transmit power, and bandw manager. If single 802.3bt class 6 power supplies are used, Wi-Fi: - If no USB port or IoT card slot is used, the number o - If the USB port or IoT card slots are used, the numbe affected. For details, contact your product manager. Wired ports: Two 10GE electrical ports and the SFP+ c working, the other is unavailable. Other ports: Both one USB port and two IoT card slots number of spatial streams, transmit power, and bandw manager. 802.3at power supply description If dual 802.3at class 6 power supplies are used, Wi-Fi: If no USB port or IoT card slot is used, the radio powe - Dual-radio mode: 2.4 GHz (2x2) + 5 GHz (4x4) - Triple-radio mode: 2.4 GHz (2x2) + 5 GHz low band - Dual-radio + independent scanning radio: 2.4 GHz If the USB port or IoT card slots are used, the number affected. For details, contact your product manager. Wired ports: The rate of both 10GE electrical ports is Other ports: The 2.5 W USB and IoT card is mutually e unavailable. The IoT card takes precedence. If the USB transmit power, and bandwidth may be affected. For If single 802.3at class 6 power supplies are used, Wi-Fi: If no USB port or IoT card slot is used, the radio powe - Dual-radio mode: 2.4 GHz (2x2) + 5 GHz (4x4) - Triple-radio mode: 2.4 GHz (2x2) + 5 GHz low band - Dual-radio + independent scanning radio: 2.4 GHz If the USB port or IoT card slots are used, the number affected. For details, contact your product manager. Wired ports: Two 10GE electrical ports provide a rate combo ports. When one of them is working, the other Other ports: The 2.5 W USB and IoT card is mutually e unavailable. The IoT card takes precedence. If the USB (2x2) + 5 GHz (2x2) mode. For details, contact your pr DC power supply description No function is restricted.

Item	Description
	• **D: data link exception**: indicates that data links of RUs have not been established. Check the network connection between the AC and RUs.
Scene	Effective scenario profile on the AP. To configure this parameter, run the **scene** command. **-** indicates that no scenario profile is configured.
Total	Total number of queried APs.

Table 11-5 AP state list

AP State	Description	Possible Cause	Handling Suggestion
commit-failed (cmtfa)	WLAN service configurations fail to be delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are performed for the AP. If the link between the AP and AC is disconnected or the peer end has no response, the AP enters the commit-failed state.	Check the network connection.
committing (cmt)	WLAN service configurations are being delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are being delivered to the AP. During this process, the AP is in committing state.	This is a normal state, and no action is required.
config (cfg)	WLAN service configurations are being delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. During this process, the AP is in config state.	This is a normal state, and no action is required.

AP State	Description	Possible Cause	Handling Suggestion
config-failed (cfgfa)	WLAN service configurations fail to be delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. If the configuration delivery fails due to various reasons (such as link disconnection), the AP enters the config-failed state.	Check the network connection.
download (dload)	An AP is in upgrade state.	When an AP is performing an upgrade, it enters the download state.	When the AP upgrade is complete, check the AP state.
fault	An AP fails to go online.	An AP fails to go online, which is usually caused by the following: • The AP fails to obtain an IP address or obtains an incorrect IP address. • The network between the AP and AC is faulty. • The AP fails to be authenticated. • The number of APs on an AC has reached the maximum value. • The AP is faulty. • In dual-link cold backup or N+1 backup scenario, if the link between the active and standby ACs is established properly, an AP that goes online on the active AC is in fault state on the standby AC.	Handle the AP online failure. For details, see **An AP Fails to Go Online on the AC** in the *Troubleshooting Guide*.

AP State	Description	Possible Cause	Handling Suggestion
idle	It is the initialization state of an AP before it establishes a link with the AC for the first time.	When an AP has not established a CAPWAP link with the AC, the MAC address and SN of an AP that is added offline are different from the actual MAC address and SN of the AP, or the AC cannot manage an AP due to license resource insufficiency, the AP enters the idle state.	Perform the following operations. Check whether the AP is connected to the network. If the AP connection is normal, go to next step. Check the MAC address and SN of the AP that is added offline are different from the actual MAC address and SN of the AP. If not, perform the following operations: 1. Run the **display ap all** command to check AP information. 2. Run the **undo ap** { **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** } command to delete the AP. 3. Run the **ap-id** *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }] or **ap-mac** *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*] command to add correct AP information. If the fault persists, expand the license capacity. Note that RUs managed by the AC do not occupy

AP State	Description	Possible Cause	Handling Suggestion
			license resources of the AC.
name-conflicted (namec)	The name of an AP conflicts with that of an existing AP.	The name of an AP conflicts with the name of another AP that has been online on the same AC.	Run the **ap-rename ap-id** *ap-id* **new-name** *ap-new-name* command to change the AP name.
normal (nor)	An AP is working properly.	An AP successfully goes online on an AC.	This is a normal state, and no action is required.
standby (stdby)	An AP is in normal state on the standby AC.	In the HSB scenario, if the link between the master and backup ACs is established properly, an AP is in standby state on the backup AC and in normal state on the master AC.	This is a normal state, and no action is required.
ver-mismatch (vmiss)	The version of an AP does not match that of an AC on which the AP is about to go online.	The versions of the AP and AC do not match.	Log in to Huawei technical support website and download the release notes. Based on the version mapping, upgrade the AP or AC to the matching version. • Enterprise technical support website: **https://support.huawei.com/enterprise** • Carrier technical support website: **https://support.huawei.com**

AP State	Description	Possible Cause	Handling Suggestion
countryCode-mismatch (cmiss)	The country codes of the AP and AC do not match.	The AP's current version does not support the country code configured on the AC. The country code of the AP is locked, and the country code configured on the AC is not supported.	The AP does not support the country code. Upgrade the AP or modify the country code configuration on the AC. The country code of the AP is locked. Replace the AP or change the country code on the AC to be the same as that of the AP.
type-mismatch (tmiss)	The AP type does not match that configured on the AC.	The AP type configured on the AC did not match the actual AP type.	Change the AP type configured on the AC.
unauth	An AP is not authenticated.	The AP fails to be authenticated.	Run the **display ap unauthorized record** command to query authenticated APs. Run the **ap-confirm** command to confirm unauthenticated APs and allow them to go online.

11.1.54 display ap blacklist

Function

The **display ap blacklist** command displays the AP blacklist.

Format

display ap blacklist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays APs in the blacklist. These APs are not allowed to go online on the AC. If an AP is online on the AC but is in the blacklist, the AP is brought offline.

Example

Display the AP blacklist.

```
<HUAWEI> display ap blacklist
------------------------------------------------------------------------------
ID     MAC
------------------------------------------------------------------------------
0      xxxx-xxxx-xxxx
------------------------------------------------------------------------------
Total: 1
```

Table 11-6 Description of the **display ap blacklist** command output

Item	Description
ID	ID of the MAC address in the AP blacklist. The ID is generated automatically when the MAC address is specified.
MAC	MAC addresses of the APs that are not allowed to connect to the AC. To configure this parameter, run the **ap blacklist** command.

11.1.55 display ap config-info

Function

The **display ap config-info** command displays AP configuration.

Format

display ap config-info { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays configuration of the AP with a specified name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Displays configuration of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap config-info** command to view AP configuration information, including the basic configuration, radio configuration, VAP configuration, and profile configuration.

Example

Display the configuration of the AP **ap1**.

```
<HUAWEI> display ap config-info ap-name ap1
-------------------------------------------------------------------------------
AP MAC                          : 00e0-fcxx-xxxx
AP SN                          : 2150083089xxxxxxxxx
AP type                        : APxxxx
AP name                         : ap1
AP group                       : default
AP branch group                 :
Country code                    : CN
Scene                          : multi-partition-cross-room
-------------------------------------------------------------------------------
Radio 0 configurations:
 Radio enable                   : yes
 Work mode                      : normal
 WDS  mode                      : -
 Mesh mode                      : -
 Radio band                     : 2.4G
 Radio type                     : 11ax
 Flexible radio switch          : on
 Config channel/bandwidth       : -/20M
 Actual channel/bandwidth       : 11/20M
 Config EIRP                    : 127
 Actual EIRP                    : 31
 Maximum EIRP                    : 31
 CCA threshold(dBm)              : -75
 RX sensitivity(dBm)            : -100
 Beacon interval(TUs)            : 60
 Dynamic EDCA                   : enable
 Station load balance sta-number start threshold          : 10
 Station load balance sta-number gap threshold(number)    : 3
 Smart roam standing SNR threshold(dB)                    : 20
 Smart roam SNR quick-kickoff-threshold(dB)               : 15
 Radio Calibration DCA 5G bandwidth                       : 40Mhz
 Radio Calibration TPC threshold(dBm):                    : -60
 Radio Calibrate grouping interference threshold(dBm)     : -70
 Radio Calibration maximum 2.4G calibration TX power(dBm) : 127
 Radio Calibration maximum 5G calibration TX power(dBm)   : 127
```



```
 Radio Calibration minimum 2.4G calibration TX power(dBm)  : 9
 Radio Calibration minimum 5G calibration TX power(dBm)    : 12

 VAP configurations:
  WLAN ID 1:
   SSID                      : employee
   Forward mode              : direct-forward
   Authen mode               : WPA/WPA2-PSK
   Encrypt mode              : AES
   Service vlan              : 3
   Deny-broadcast-probe      : disable
   Active dull client        : disable
   Force active dull client  : disable
   Association timeout(min)  : 1
-------------------------------------------------------------------------------
Radio 1 configurations:
 Radio enable                : yes
 Work mode                   : normal
 WDS  mode                   : -
 Mesh mode                   : -
 Radio band                  : 5G
 Radio type                  : 11ax
 Flexible radio switch       : on
 Config channel/bandwidth    : -/20M
 Actual channel/bandwidth    : 157/20M
 Config EIRP                 : 127
 Actual EIRP                 : 30
 Maximum EIRP                : 30
 CCA threshold(dBm)          : -75
 RX sensitivity(dBm)         : -100
 Beacon interval(TUs)        : 100
 Dynamic EDCA                : enable
 Station load balance sta-number start threshold       : 10
 Station load balance sta-number gap threshold(number) : 3
 Smart roam standing SNR threshold(dB)                 : 20
 Smart roam SNR quick-kickoff-threshold(dB)            : 15
 Radio Calibration DCA 5G bandwidth                    : 80Mhz
 Radio Calibration TPC threshold(dBm)                  : -35
 Radio Calibrate grouping interference threshold(dBm)  : -70
 Radio Calibration maximum 2.4G calibration TX power(dBm)  : 127
 Radio Calibration maximum 5G calibration TX power(dBm)    : 127
 Radio Calibration minimum 2.4G calibration TX power(dBm)  : 9
 Radio Calibration minimum 5G calibration TX power(dBm)    : 12

 VAP configurations:
  WLAN ID 1:
   SSID                      : employee
   Forward mode              : direct-forward
   Authen mode               : WPA/WPA2-PSK
   Encrypt mode              : AES
   Service vlan              : 3
   Deny-broadcast-probe      : disable
   Active dull client        : disable
   Association timeout(min)  : 1
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
AP system profile         : default
Regulatory domain profile : default
WIDS profile              : default
BLE profile               :
Site code                 :
AP location               :
Broadcaster content
  UUID                    : -
  Major                   : -
  Minor                   : -
  Reference RSSI          : -
Domain name               :
Ap pki profile            :
```



```
AP wired port profile
 Interface FE0             : default
 Interface FE1             : default
 Interface FE2             : default
 Interface FE3             : default
 Interface GE0             : default
 Interface GE1             : default
 Interface GE2             : default
 Interface GE3             : default
 Interface GE4             : default
 Interface GE5             : default
 Interface GE6             : default
 Interface GE7             : default
 Interface GE8             : default
 Interface GE9             : default
 Interface GE10            : default
 Interface GE11            : default
 Interface GE12            : default
 Interface GE13            : default
 Interface GE14            : default
 Interface GE15            : default
 Interface GE16            : default
 Interface GE17            : default
 Interface GE18            : default
 Interface GE19            : default
 Interface GE20            : default
 Interface GE21            : default
 Interface GE22            : default
 Interface GE23            : default
 Interface GE24            : default
 Interface GE25            : default
 Interface GE26            : default
 Interface GE27            : default
 Interface MultiGE0        : default
 Interface MultiGE2        : default
 Interface MultiGE3        : default
 Interface MultiGE4        : default
 Interface MultiGE5        : default
 Interface MultiGE6        : default
 Interface MultiGE7        : default
 Interface XGE0            : default
 Interface XGE1            : default
 Interface XGE2            : default
 Interface XGE3            : default
 Interface XGE4            : default
 Interface XGE5            : default
 Interface XGE6            : default
 Interface XGE7            : default
 Interface Eth-trunk0      : default
 Interface Eth-trunk1      : default
 Radio 0
  Radio 2.4G profile       : default
  Radio 5G profile         :
  VAP profile              :
  Mesh profile             :
  WDS profile              :
  Mesh whitelist profile   :
  WDS whitelist profile    :
  Location profile         :
 Radio switch              : enable
 Channel                   : -
 Channel bandwidth         : 20mhz
 EIRP(dBm)                 : 127
 Antenna gain(dB)          : -
 Coverage distance(100 m)  : 3
 Work mode                 : normal
 Flexible radio switch     : on
 Radio frequency           : 2.4G
 Spectrum analysis         : disable
```



```
 Channel monitor           : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
 Auto channel select       : enable
 Auto bandwidth select     : disable
 Auto transmit power select: enable
 Reference data-analysis   : enable
 Reference 3d-data         : enable
 Radio 1
  Radio 5G profile         : default
  VAP profile              :
  Mesh profile             :
  WDS profile              :
  Mesh whitelist profile   :
  WDS whitelist profile    :
  Location profile         :
 Radio switch              : enable
 Channel                   : -
 Channel bandwidth         : 20mhz
 EIRP(dBm)                 : 127
 Antenna gain(dB)          : -
 Coverage distance(100 m)  : 3
 Work mode                 : normal
 Flexible radio switch     : on
 Radio frequency           : 5G
 Spectrum analysis         : disable
 Channel monitor           : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
 Auto channel select       : enable
 Auto bandwidth select     : disable
 Auto transmit power select: enable
 Reference data-analysis   : enable
 Reference 3d-data         : enable
 Interference visualization: disable
Card 1
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
 Extended Port             : -
Card 2
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
 Extended Port             : -
Card 3
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
 Extended Port             : -
Card usb
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
```



```
Extended Port          : -
-------------------------------------------------------------------------------
```

Table 11-7 Description of the **display ap config-info** command output

Item	Description
AP MAC	MAC address of an AP.
AP SN	SN of an AP.
AP type	AP type.
AP name	AP name. To configure this parameter, run the **ap-name (AP view)** or **ap-rename** command.
Domain name	Default domain name suffix of the AP. To configure this parameter, run the **ip domain-name** command.
AP group	AP group. To configure this parameter, run the **ap-group (AP view)** or **ap-regroup** command.
Country code	Country code. To configure this parameter, run the **country-code** command.
Scene	Effective scenario profile on the AP. To configure this parameter, run the **scene** command.
Radio x configurations	Radio configuration.
Radio enable	Whether a radio is enabled. To configure this parameter, run the **radio disable** command.
Work mode	Working mode of a radio. To configure this parameter, run the **work-mode** command.
WDS mode	WDS mode. To configure this parameter, run the **wds-mode** command.
Mesh mode	Mesh role of a radio. To configure this parameter, run the **mesh-role** command.

Item	Description
Radio band	Frequency band of a radio. To configure this parameter, run the **frequency** command.
Radio type	Protocol type of a radio.
Flexible radio switch	Whether the DFA function of a radio is enabled. To configure this parameter, run the **calibrate flexible-radio disable** command.
Config channel/bandwidth	Configured AP channel and bandwidth. To configure this parameter, run the **channel** command.
Actual channel/bandwidth	Actual AP channel and bandwidth.
Config EIRP	Transmit power of a radio configured in the radio profile. To configure this parameter, run the **eirp** command.
Actual EIRP	Actual transmit power of a radio.
Maximum EIRP	Maximum transmit power of a radio.
Radio Calibration DCA 5G bandwidth	5 GHz radio calibration bandwidth configuration obtained from the bound scenario profile. To configure this parameter, run the **scene** command.
Radio Calibration TPC threshold(dBm)	Radio calibration power configuration obtained from the bound scenario profile. To configure this parameter, run the **scene** command.
Radio Calibrate grouping interference threshold(dBm)	Interference threshold of a calibration group obtained from the bound scenario profile. To configure this parameter, run the **scene** command.
CCA threshold(dBm)	CCA threshold for AP radios. To configure this parameter, run the **cca-threshold** command.

Item	Description
RX sensitivity(dBm)	Receiver sensitivity. To configure this parameter, run the **rx-sensitivity** command.
Beacon interval(TUs)	Interval at which an AP sends Beacon frames. To configure this parameter, run the **beacon-interval** command.
Dynamic EDCA	Enabling status of dynamic EDCA obtained from the bound scenario profile. To configure this parameter, run the **scene** command.
Station load balance sta-number start threshold	Start threshold for dynamic load balancing based on the number of STAs. To configure this parameter, run the **sta-load-balance dynamic sta-number start-threshold** command.
Station load balance sta-number gap threshold(number)	Load difference threshold for dynamic load balancing based on the number of STAs. To configure this parameter, run the **sta-load-balance dynamic sta-number gap-threshold** command.
Smart roam standing SNR threshold(dB)	SNR threshold for smart roaming. To configure this parameter, run the **smart-roam roam-threshold { snr | rate }** command.
Smart roam SNR quick-kickoff-threshold(dB)	SNR threshold for quickly disconnecting STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold** command.
Radio Calibration maximum 2.4G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 2.4 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power** command.

Item	Description
Radio Calibration maximum 5G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 5 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power radio-5g** command.
Radio Calibration minimum 2.4G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 2.4 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power** command.
Radio Calibration minimum 5G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 5 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power radio-5g** command.
VAP configurations	VAP configuration. VAP configuration is displayed only after a VAP profile is referenced by the AP.
WLAN ID 1	WLAN ID of a VAP. To configure this parameter, run the **vap-profile** command.
SSID	SSID name. To configure this parameter, run the **ssid** command.
Forward mode	Forwarding mode. To configure this parameter, run the **forward-mode** command.
Authen mode	Authentication mode.
Encrypt mode	Encryption mode.
Service vlan	Effective service VLAN.
Deny-broadcast-probe	Whether an AP is configured not to respond to broadcast Probe Request frames. To configure this parameter, run the **deny-broadcast-probe enable** command.

Item	Description
Active dull client	Whether the function of preventing terminals from entering energy-saving mode is enabled. To configure this parameter, run the **active-dull-client enable** command.
Force active dull client	Whether the function of forcibly preventing terminals from entering power-saving mode is enabled. To configure this parameter, run the **active-dull-client force enable** command.
Association timeout(min)	Specifies the association aging time of STAs. To configure this parameter, run the **association-timeout** command.
AP system profile	Name of the referenced AP system profile. To configure this parameter, run the **ap-system-profile (AP group view and AP view)** command.
Regulatory domain profile	Name of the referenced regulatory domain profile. To configure this parameter, run the **regulatory-domain-profile** command.
WIDS profile	Name of the referenced WIDS profile.
BLE profile	Name of the referenced BLE profile. To configure this parameter, run the **ble-profile (AP group view and AP view)** command.
AP location	Installation position of an AP. To configure this parameter, run the **location** command.
UUID	UUID of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP view)** command.

Item	Description
Major	Major field of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP view)** command.
Minor	Minor field of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP view)** command.
Reference RSSI	Reference RSSI of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP view)** command.
Ap pki profile	Bound AP PKI realm profile. To configure this parameter, run the **ap-pki-profile** command.
AP wired port profile	Name of the referenced AP wired port profile. To configure this parameter, run the **wired-port-profile (AP group view and AP view)** command.
Interface *interface-name*	Interface name and number.
Radio x	Radio.
Radio 2.4G profile	Name of the referenced 2G radio profile. To configure this parameter, run the **radio-2g-profile** command.
Radio 5G profile	Name of the referenced 5G radio profile. To configure this parameter, run the **radio-5g-profile** command.

Item	Description
VAP profile	Name of the referenced VAP profile. The displayed format is "VAP ID:VAP profile name (service VLAN defined when binding to the VAP profile, single VLAN, or VLAN pool)." To configure this parameter, run the **vap-profile** command.
Mesh profile	Name of the referenced Mesh profile. To configure this parameter, run the **mesh-profile radio** command.
WDS profile	Name of the referenced WDS profile. To configure this parameter, run the **wds-profile radio** command.
Mesh whitelist profile	Mesh whitelist profile referenced by an AP group. To configure this parameter, run the **mesh-whitelist-profile (AP group radio view or AP radio view)** command.
WDS whitelist profile	WDS whitelist profile referenced by an AP group. To configure this parameter, run the **wds-whitelist-profile (AP group radio view or AP radio view)** command.
Location profile	Name of the referenced location profile. To configure this parameter, run the **location-profile** command.
Radio switch	Whether a radio is enabled. To configure this parameter, run the **radio disable** command.
Channel	Working channel of a radio. To configure this parameter, run the **channel** command.
Channel bandwidth	Working bandwidth of a radio. To configure this parameter, run the **channel** command.
EIRP(dBm)	Transmit power of a radio, in dBm. To configure this parameter, run the **eirp** command.

Item	Description
Antenna gain(dB)	Antenna gain of a radio, in dB. To configure this parameter, run the **antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter, in the unit of 100 m. To configure this parameter, run the **coverage distance** command.
Work mode	Working mode of an AP. To configure this parameter, run the **work-mode** command.
Radio frequency	Working frequency band of a radio. To configure this parameter, run the **frequency** command.
Spectrum analysis	Whether spectrum analysis is enabled. To configure this parameter, run the **spectrum-analysis enable** command.
Channel monitor	Whether the function of monitoring the status of all channels is enabled. To configure this parameter, run the **channel-monitor enable** command.
WIDS device detect	Whether wireless device detection is enabled. To configure this parameter, run the **wids device detect enable** command.
WIDS attack detect	Whether attack detection is enabled. To configure this parameter, run the **wids attack detect** command.
WIDS contain switch	Whether rogue device containment is enabled. To configure this parameter, run the **wids contain enable** command.
Auto channel select	Whether automatic channel selection is enabled. To configure this parameter, run the **calibrate auto-channel-select** command.

Item	Description
Auto bandwidth select	Whether automatic bandwidth selection is enabled. To configure this parameter, run the **calibrate auto-bandwidth-select** command.
Auto transmit power select	Whether automatic transmit power selection is enabled. To configure this parameter, run the **calibrate auto-txpower-select** command.
Reference data-analysis	Whether big data calibration is enabled. To configure this parameter, run the **calibrate reference data-analysis { disable | enable }** command.
Reference 3d-data	Whether 3D radio calibration is enabled. To configure this parameter, run the **calibrate reference 3d-data { disable | enable }** command.
Interference visualization	Whether the interference visualization function is enabled. To configure this parameter, run the **interference-visualization enable** command.
Card 1/Card 2/Card 3/Card usb	IoT card.
Card connect type	Communication connection type between IoT cards and APs. To configure this parameter, run the **card connect-type** command.
Baud rate	Baud rate used for communication between an IoT card and the AP. To configure this parameter, run the **baud-rate** command.
Wired port profile	Bound AP wired port profile. To configure this parameter, run the **wired-port-profile (IoT card interface view)** command.

Item	Description
Iot profile	Bound IoT profile. To configure this parameter, run the **iot-profile (IoT card interface view)** command.
Protocol Type	Communication protocol between the AP and host computer.
First Port	Source port for the first channel.
Extended Port	Source port for the extended channel.

11.1.56 display ap configurable channel

Function

The **display ap configurable channel** command displays the configurable channels supported by a specified AP.

Format

display ap configurable channel { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays configurable channels supported by the AP with the specified name.	The AP name must exist.
ap-id *ap-id*	Displays configurable channels supported by the AP with the specified ID.	The AP ID must exist.
radio *radio-id*	Displays configurable channels supported by the specified radio.	The radio ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Available wireless channels and power levels vary in different countries or regions. The country code configuration allows you to specify channels that can available

on WLANs in the local country or region. You can run this command to view configurable channels supported by a specified AP.

Example

Display configurable channels supported by the AP named **test**.

```
<HUAWEI> display ap configurable channel ap-name test
2.4G 20M : 1,2,3,4,5,6,7,8,9,10,11,12,13.
2.4G 40M+: 1,2,3,4,5,6,7,8,9.
2.4G 40M-: 5,6,7,8,9,10,11,12,13.
5G   20M : 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,157,161,165.
5G   40M+: 36,44,52,60,100,108,116,124,132,149,157.
5G   40M-: 40,48,56,64,104,112,120,128,136,153,161.
5G   80M : 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,149,153,157,161.
5G  160M : 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128.
5G 80+80M: 36+106, 36+122, 36+155, 40+106, 40+122, 40+155, 44+106, 44+122,
           44+155, 48+106, 48+122, 48+155, 52+106, 52+122, 52+155, 56+106,
           56+122, 56+155, 60+106, 60+122, 60+155, 64+106, 64+122, 64+155,
           100+42, 100+58, 100+155, 104+42, 104+58, 104+155, 108+42, 108+58,
           108+155, 112+42, 112+58, 112+155, 116+42, 116+58, 116+155, 120+42,
           120+58, 120+155, 124+42, 124+58, 124+155, 128+42, 128+58, 128+155,
           149+42, 149+58, 149+106, 149+122, 153+42, 153+58, 153+106, 153+122,
           157+42, 157+58, 157+106, 157+122, 161+42, 161+58, 161+106, 161+122.
6G   20M : 1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,
           93,97,101,105,109,113,117,121,125,129,133,137,141,145,149,153,157,
           161,165,169,173,177,181,185,189,193,197,201,205,209,213,217,221,225,
       229,233
6G   40M+: 1,9,17,25,33,41,49,57,65,73,81,89,97,105,113,121,129,137,145,153,161,
           169,177,185,193,201,209,217,225
6G   40M-: 5,13,21,29,37,45,53,61,69,77,85,93,101,109,117,125,133,141,149,157,
           165,173,181,189,197,205,213,221,229
6G   80M : 1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93,
           97,101,105,109,113,117,121,125,129,133,137,141,145,149,153,157,161,
           165,169,173,177,181,185,189,193,197,201,205,209,213,217,221
6G  160M : 1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93,
           97,101,105,109,113,117,121,125,129,133,137,141,145,149,153,157,161,165,
           169,173,177,181,185,189,193,197,201,205,209,213,217,221
```

Table 11-8 Description of the **display ap configurable channel** command output

Item	Description
2.4G 20M	Configurable 20 MHz channels supported by the AP on the 2.4 GHz frequency band.
2.4G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 2.4 GHz frequency band.
2.4G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 2.4 GHz frequency band.
5G 20M	Configurable 20 MHz channels supported by the AP on the 5 GHz frequency band.
5G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 5 GHz frequency band.
5G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 5 GHz frequency band.

Item	Description
5G 80M	Configurable 80 MHz channels supported by the AP on the 5 GHz frequency band.
5G 160M	Configurable 160 MHz channels supported by the AP on the 5 GHz frequency band.
5G 80+80M	Configurable 80+80 MHz channels supported by the AP on the 5 GHz frequency band.
5G 320M	Configurable 320 MHz channels supported by the AP on the 5 GHz frequency band.
6G 20M	Configurable 20 MHz channels supported by the AP on the 6 GHz frequency band.
6G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 6 GHz frequency band.
6G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 6 GHz frequency band.
6G 80M	Configurable 80 MHz channels supported by the AP on the 6 GHz frequency band.
6G 160M	Configurable 160 MHz channels supported by the AP on the 6 GHz frequency band.
6G 320M	Configurable 320 MHz channels supported by the AP on the 6 GHz frequency band.

11.1.57 display ap global configuration

Function

The **display ap global configuration** command displays AP global configuration.

Format

display ap global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view AP global information.

Example

Display AP global configuration.

```
<HUAWEI> display ap global configuration
------------------------------------------------------------------------------
AP auth-mode                    : MAC-auth
AP LLDP switch                  : disable
AP username/password              : -/******
AP data collection              : disable
AP data collection interval(minute): 5
------------------------------------------------------------------------------
```

Table 11-9 Description of the **display ap global configuration** command output

Item	Description
AP auth-mode	AP authentication mode. To configure this parameter, run the **ap auth-mode** command.
AP LLDP switch	Whether LLDP is enabled on an AP. To configure this parameter, run the **ap lldp enable** command.
AP username/password	User name and password for logging in to an AP. To configure this parameter, run the **ap username** command.
AP data collection	Whether data buffering is enabled on an AP. To configure this parameter, run the **ap data-collection enable** command.
AP data collection interval(minute)	AP data buffering interval. To configure this parameter, run the **ap data-collection interval** command.

11.1.58 display ap non-factory all

Function

The **display ap non-factory all** command displays Fat APs and cloud APs on the network.

Format

display ap non-factory all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the working mode of a Fit AP is switched to the Fat or cloud mode, the AP cannot be managed by the device. Fat or cloud APs detected on the current network can be displayed. Based on AP information, check whether the AP mode is switched by mistake.

Follow-up Procedure

If so, run the **ap manufacturer-config** command to switch the working mode of the AP to Fit.

Precautions

The device can detect Fat APs and cloud APs only when the following conditions are met:

- The IP address of an AP in non-Fit mode is not obtained through DHCP, or its IP address is obtained through DHCP but the AP does not obtain the AC address through the option field. In this scenario, the device can detect the AP as a non-Fit AP by the device when the AP is in the same LAN as the device.
- The IP address of an AP in non-Fit mode is obtained through DHCP, and the AP does not obtain the AC address through the option field. In this scenario, the device can detect the AP as a non-Fit AP by the device when the address for the device to manage the Fit AP is the same as the address specified in the option field.

Example

Display APs that operate in non-Fit mode on the network.

```
<HUAWEI> display ap non-factory all
Cnt: Manage FIT AP count
Mode: Actual mode/Config mode
--------------------------------------------------------------------------------------------------------------------
-------
MAC          SN              IP              Type              Mode        Cnt  Operate State    Record time
--------------------------------------------------------------------------------------------------------------------
-------
00e0-fc11-2222  **********1       10.1.1.11       AirEngine8760-X1-PRO  FAT/-       1    waiting deliver
2023-07-22 17:23:17
```



```
00e0-fc11-2233  **********2        10.1.1.12        AirEngine8760-X1-PRO   CLOUD/CLOUD  0     -
2023-07-22 17:33:17
00e0-fc11-3344  **********3        10.1.1.13        AirEngine8760-X1-PRO   CLOUD/-      0     delivered
2023-07-22 17:33:17
--------------------------------------------------------------------------------------------------------------
-------
Total: 3
```

Table 11-10 Description of the **display ap non-factory all** command output

Item	Description
MAC	MAC address of an AP in non-Fit mode.
SN	SN of an AP in non-Fit mode.
IP	IP address of an AP in non-Fit mode.
Type	Type of an AP in non-Fit mode.
Mode	Current mode and configuration mode of an AP in non-Fit mode. The configuration mode refers to the specified mode information received by the AP through DHCP Option 148. When the configuration mode is not empty, the Fit mode cannot be restored.
Cnt	Number of managed Fit APs when the AP in non-Fit mode is the leader AP.
Operate State	State of receiving the **ap manufacturer-config** command on an AP in non-Fit mode. ● waiting deliver: The command has been delivered but has not been received on the AP. ● delivered: The AP has received the command. ● -: The command is not delivered.
Record time	Latest time when the AP is detected.
Total	Total number of times APs in non-Fit mode are detected.

11.1.59 display ap offline-record

Function

The **display ap offline-record** command displays AP offline records.

Format

display ap offline-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays offline records of all APs.	-
mac *mac-address*	Displays offline records of the AP with the specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays AP offline records, helping the maintenance personnel manage and maintain the APs.

After the number of AP offline records reaches the maximum that can be stored, new records overwrite existing ones.

A maximum of five offline records can be stored for each AP.

Example

Display offline records of all APs.

```
<HUAWEI> display ap offline-record all
--------------------------------------------------------------------------------
MAC               Last offline time      Reason
--------------------------------------------------------------------------------
00e0-fc24-0080    2015-01-31/16:21:50    The AP name is modified.
00e0-fc76-e360    2015-01-31/14:02:35    The AP is replaced.
--------------------------------------------------------------------------------
Total records: 2
```

Table 11-11 Description of the **display ap offline-record** command output

Item	Description
MAC	MAC address of an AP.
Last offline time	Time when the AP went offline last time.

Item	Description
Reason	Reason why the AP goes offline. For the description of offline reasons and handling suggestions, see **Table 11-12**. For more troubleshooting methods, see **An AP Goes Offline Unexpectedly** in the *Troubleshooting Guide*.

Table 11-12 Possible reasons and suggestions for APs to go offline

Reason Why an AP Goes Offline	Suggestion
The AC country code is modified.	The AP goes offline due to normal configuration changes, and no action is required.
The AP is replaced.	The AP goes offline due to normal configuration changes, and no action is required.
Reboot by ap update reset command. The AP is reset automatically after the upgrade.	The AP resets to load the new version file after the upgrade, and no action is required.
A command is delivered to reboot an AP.	The AC delivers a reboot command to the AP, and no action is required.
An AP is deleted.	The AP is deleted on the AC, and no action is required.
The license expires.	Apply for a new license. For details, see *WLAN License Usage Guide*.
Insufficient license resources.	Choose one of the following handling suggestions based on the networking: • If license control is deployed, check whether the link between the license server and client is disconnected. If so, restore the link. • If N+1 or dual-link backup is deployed, check whether the active and standby link is disconnected. If so, restore the link. • If the number of APs on the network exceeds the total number of license resources, apply for a new license.
The AP is added to the blacklist.	Check whether the AP needs to be added to the blacklist.

Reason Why an AP Goes Offline	Suggestion
A CAPWAP tunnel is faulty (due to inconsistent link IDs).	The AP will automatically attempt to recover the link, and no action is required.
The DTLS configuration of the CAPWAP tunnel changes.	The AP goes offline due to normal configuration changes, and no action is required.
The AP's factory settings are restored.	The AP goes offline due to normal configuration changes, and no action is required.
The radio type is inconsistent between the AC and AP.	Run the **display ap config-info** command to verify the AP radio configuration.
Heartbeat packet transmission for the CAPWAP data tunnel between the AC and AP times out.	Check the intermediate network between the AP and AC.
Heartbeat packet transmission for the CAPWAP control tunnel between the AC and AP times out.	Check the intermediate network between the AP and AC.
The dual-link networking configuration is modified.	The configuration change causes the AP to automatically reboot, and no action is required.
The AP name is modified.	The AP goes offline due to normal configuration changes, and no action is required.
The AP group name is modified.	The AP goes offline due to normal configuration changes, and no action is required.
The management VLAN is modified.	The AP goes offline due to normal configuration changes, and no action is required.
AP provisioning parameters are set.	The AP goes offline due to normal configuration changes, and no action is required.
The CAPWAP source IP address is deleted.	The AP goes offline due to normal configuration changes, and no action is required.
The central AP goes offline.	Check the reason why the central AP goes offline.
The central AP proactively reboots RUs.	The AP goes offline due to normal configuration changes, and no action is required.

Reason Why an AP Goes Offline	Suggestion
The AP is powered off and restarts.	If the AP restarts repeatedly, check whether the AP power supply mode matches the actual power supply.
An internal error (KP) occurs.	Contact technical support personnel.
An internal error (VOS signal error) occurs.	Contact technical support personnel.
An internal error (forwarding error monitored by MFPI) occurs.	Contact technical support personnel.
An internal error (PKO error monitored by MSC) occurs.	Contact technical support personnel.
An internal error (reset due to timer expiration) occurs.	Contact technical support personnel.
An internal error (reset of the write CPLD register) occurs.	Contact technical support personnel.
The reset button is pressed to reset the AP.	Check whether the AP is manually reset.
The AP restarts due to a CANBUS reset.	Contact technical support personnel.
The AP restarts due to AP interference.	Contact technical support personnel.
The AP restarts due to a chip exception. The AP restarts due to a firmware exception.	Contact technical support personnel.
The CAPWAP sensitive-info PSK is modified.	The configuration change causes the AP to automatically reboot, and no action is required.
The CAPWAP integrity-check PSK is modified.	The configuration change causes the AP to automatically reboot, and no action is required.
The country code is inconsistent on the AC and AP.	Check the country code configuration on the AC and AP.

Reason Why an AP Goes Offline	Suggestion
The AP is forcibly disconnected.	Check the fault based on the possible causes, which may be: ● CAPWAP resources are insufficient. ● The access interface of the AP is changed. ● The Eth-Trunk connected to the AP is deleted. If the fault persists, contact technical support personnel.
The wideband status change.	The AP goes offline due to normal configuration changes, and no action is required.
Reset for a configuration delivery failure.	Check network connectivity. If no problem is found, contact technical support personnel.
Reboot for the branch group of AP change.	The AP goes offline due to normal configuration changes, and no action is required.
The AC license expires.	Re-activate the AC license.
A CAPWAP tunnel is faulty (due to a CAPWAP link entry verification failure).	The AP will automatically attempt to recover the link, and no action is required.
Batch delete	Check whether the active AC runs properly. When the active AC is restored, the AP switches to this active AC to go online.
Switch service radio to proxy scanning radio.	The configuration change causes the AP to automatically reboot, and no action is required.
Switch proxy scanning radio to service radio.	The configuration change causes the AP to automatically reboot, and no action is required.
The AP cloud license expires.	Purchase a new license and load it to iMaster NCE-Campus.
The device has been disconnected from the iMaster NCE-Campus for more than 90 days.	Verify the iMaster NCE-Campus address configured on the AC, and check network connectivity.
The device is deleted from the iMaster NCE-Campus.	No action is required.

Reason Why an AP Goes Offline	Suggestion
The iMaster NCE-Campus does not deliver AP information.	1. Verify that AP information is correctly added to iMaster NCE-Campus, the AP is associated with the AC, and the AC is online. 2. Verify the iMaster NCE-Campus address configured on the AC, and check network connectivity. 3. Check whether iMaster NCE-Campus fails to deliver AP information. If so, manually deliver AP information again.
An internal error (Reset for firmware abnormal) occurs.	Contact technical support personnel.
An internal error (Reset for abnormal network port self-healing) occurs.	Contact technical support personnel.
An internal error (Reset for the forcible AP disconnection in specific scenarios) occurs.	Contact technical support personnel.
An internal error (Reset for slow task switching) occurs.	Contact technical support personnel.
An internal error (Reset for MFPI detect CAP PBUF use out) occurs.	Contact technical support personnel.
An internal error (Reset for ap abnormal self-healing) occurs.	Contact technical support personnel.
An internal error (Reset for exception(redis-server exit)) occurs.	Contact technical support personnel.
An internal error (Reset for exception(confd exit)) occurs.	Contact technical support personnel.
An internal error (Reset for exception(callhome exit)) occurs.	Contact technical support personnel.
An internal error (Reset for an abnormal process) occurs.	Contact technical support personnel.
N+1 switchover of APs.	No action is required.
An internal error (Reset for an NP heartbeat message exception) occurs	Contact technical support personnel.
An internal error (exceed the extreme temperature) occurs.	Take proper measures to lower the ambient temperature, for example, by lowering the air conditioner temperature and ventilate the equipment room.

Reason Why an AP Goes Offline	Suggestion
An internal error (memory use out) occurs.	Contact technical support personnel.
An internal error (dophi-server exit) occurs.	Contact technical support personnel.
An internal error (Wi-Fi SDK self-healing failure) occurs.	Contact technical support personnel.
Reconnect by command.	No action is required.
Reset for the radio mode change.	No action is required.
Reset for RTU license activation.	No action is required.
Reset for an overdue demo license.	No action is required.
Reset for insufficient power supply.	Contact technical support personnel.
An internal error (Reset for an unexpected exit of the WPC process) occurs.	Contact technical support personnel.
Cloud licenses expire, and local license resources are insufficient	Expand the license capacity (RUs do not occupy license resources).
Incompatible DTLS version or encryption algorithm	Upgrade the AP version, or run the **capwap dtls version1.0 enable** and **capwap dtls cbc enable** commands to enable compatibility with earlier DTLS versions.
The CAPWAP DTLS authentication configuration of the AP is changed	The AP goes offline due to configuration changes, and no action is required.

11.1.60 display ap online-fail-record

Function

The **display ap online-fail-record** command displays AP online failure records.

Format

display ap online-fail-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays online failure records of all APs.	-

Parameter	Description	Value
mac *mac-address*	Displays online failure records of the AP with the specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an AP fails to go online on the AC, you can run this command to check the failure reason, which helps locate the fault.

After the number of AP online failure records reaches the maximum that can be stored, new records overwrite existing ones.

A maximum of five online failure records can be stored for each AP.

Example

Display online failure records about the AP with the MAC address 00e0-fcb1-56a0.

```
<HUAWEI> display ap online-fail-record mac 00e0-fcb1-56a0
--------------------------------------------------------------------------------
MAC            Last fail time       Reason
--------------------------------------------------------------------------------
00e0-fcb1-56a0  2015-01-20/15:48:06  The AP is added to the AP blacklist.
--------------------------------------------------------------------------------
Total records: 1
```

Table 11-13 Description of the **display ap online-fail-record** command output

Item	Description
MAC	MAC address of the AP that fails to go online.
Last fail time	Time of the AP online failure.
Reason	Reason why the AP fails to go online. For details about going-online failure causes and handling suggestions, see **Table 11-14**. For more troubleshooting methods, see **An AP Fails to Go Online on the AC** in the *Troubleshooting Guide*.

Table 11-14 Possible causes and suggestions for APs' failures to go online

Reason Why an AP Fails to Go Online	Suggestion
Insufficient license resources.	Expand the license capacity. Note that RUs do not occupy license resources of the AC. For details, see *WLAN License Usage Guide*.
The AP is not in the SN whitelist.	Run the **ap whitelist sn** *ap-sn1* [**to** *ap-sn2*] command to add the AP to the whitelist or run the **ap-confirm** command to enable the AP to pass authentication.
The AP is not in the MAC whitelist.	Run the **ap whitelist mac** *ap-mac1* [**to** *ap-mac2*] command to add the AP to the whitelist or run the **ap-confirm** command to enable the AP to pass authentication.
The AP is added to the AP blacklist.	Check whether the AP needs to be added to the blacklist. To delete the AP from the blacklist, run the **undo ap blacklist** command.
The MAC address and SN of the AP do not match.	Check whether the MAC address and SN of the AP match.
DTLS negotiation for CAPWAP tunnel setup fails.	Check whether the PSK used for DTLS encryption is correctly configured.
DTLS negotiation failed, because of negotiation timeout or inconsistent PSKs on two ends.	• Check whether the shared keys of the AC and AP are the same. If not, change them to the same. Alternatively, enable the function of establishing CAPWAP DTLS sessions in none authentication mode so that the APs can obtain security credentials. After the APs go online, disable this function immediately in order to prevent unauthorized APs from going online. • Check whether ping packets are normal on the network. If not, negotiation timeout occurs because of a network exception during the DTLS negotiation. In this case, check the network. • If this fault persists, contact technical support personnel.

Reason Why an AP Fails to Go Online	Suggestion
CAPWAP tunnel negotiation fails.	Check network connectivity. If no problem is found, contact technical support personnel.
APs cannot go online during data backup.	Wait until backup is complete.
The upgrade fails.	Run the **display ap update configuration** command to check whether the AP's upgrade file is correct. If so, rectify the fault by referring to **Fit AP Upgrade Fails** in the *Troubleshooting Guide*.
The CAPWAP tunnel fails to be established.	Check network connectivity. If no problem is found, contact technical support personnel.
The configuration fails to be delivered.	The device attempts to deliver the configuration again. If the failure persists: 1. Check whether the AC and AP can ping each other. If the network is disconnected or a large number of packets are lost, check the intermediate network. 2. Check whether the MTU between the AC and AP is correctly configured. Assume that the MTU of the intermediate network is 1500 bytes. Run the **ping -a** *<AC CAPWAP source IP>* **-s** *1472* **-f** *<AP IP>* command on the AC to check whether the ping operation succeeds. If packet loss occurs, run the **mtu** (AP system profile view) command to change the MTU of the AP to be the same as the MTU of the intermediate network. 3. Check whether the AC and AP can properly send and receive packets, whether the queue usage exceeds the threshold, and whether packet loss or any loop occurs on interfaces. If this fault persists, contact technical support personnel.

Reason Why an AP Fails to Go Online	Suggestion
The versions of the AP and AC do not match.	Log in to Huawei technical support website and download the release notes. Based on the version mapping, upgrade the AP or AC to the matching version. • Enterprise technical support website: **https://support.huawei.com/enterprise** • Carrier technical support website: **https://support.huawei.com**
• The AC does not support the AP type. • Unsupported AP type, AC version may need to be upgraded.	Replace the AP with that supported by the AC or replace the AC with one that supports this AP type. To enable an AC to manage APs that are new in a later version, you can manually add AP types. For details, see **Enabling a WAC to Manage New APs Running Later Versions**.
The AP name conflicts.	Run the **ap-rename** command to rename the AP.
The number of central APs reaches the upper limit.	Check whether the number of central APs reaches the maximum value.
The number of common APs reaches the upper limit.	Check whether the number of common APs reaches the maximum value. If the number of normal APs is smaller than the maximum, to allow the AP to go online, run the **undo ap** command to delete APs that are not in normal state to release resources.
The central AP is not in normal state.	Run the **display ap** command to check the central AP status and take measures accordingly.
The CAPWAP sensitive-info PSK is different on the two ends of the CAPWAP tunnel.	Ensure that the PSK for encrypting CAPWAP sensitive information is the same on the AP and AC. Alternatively, enable the AP to set up a DTLS session with the AC using the default PSK.
The CAPWAP integrity-check PSK is different on the two ends of the CAPWAP tunnel.	Ensure that the PSK for checking CAPWAP packet integrity is the same on the AP and AC. Alternatively, enable the AP to set up a DTLS session with the AC using the default PSK.

Reason Why an AP Fails to Go Online	Suggestion
The configured and reported AP types are different. The real AP type is *XXXX*. The type ID carried by the AP is different from that configured on the AC.	After the **undo AP** command is run to delete an AP, the system cannot obtain the AP type and displays a message "The configured and reported AP types are different." In this case, ensure that the configured AP type is the same as the reported one.
The AC license is not active.	Activate the AC license.
Too many APs go online concurrently, leading to a failure to create sufficient DBSS interfaces.	No action is required. The APs will attempt to go online again. If the APs still fail to go online, contact technical support personnel.
The country codes of the AP and AC are inconsistent, and the country code of the AP is locked.	The country code of some AP models cannot be modified. For example, an AP model with the suffix -US is used only in the United States, and its country code is fixed as US. Configure the country code on the AC to be the same as that on the AP.
The AP cloud license expires.	Purchase a new license and load it to iMaster NCE-Campus.
The device has been disconnected from the iMaster NCE-Campus for more than 90 days.	Verify the iMaster NCE-Campus address configured on the AC, and check network connectivity.
The device is deleted from the iMaster NCE-Campus.	No action is required.
The iMaster NCE-Campus does not deliver AP information.	1. Verify that AP information is correctly added to iMaster NCE-Campus, the AP is associated with the AC, and the AC is online. 2. Verify the iMaster NCE-Campus address configured on the AC, and check network connectivity. 3. Check whether iMaster NCE-Campus fails to deliver AP information. If so, manually deliver AP information again.
Configuration synchronization is in progress, leading to the system busy.	No action is required.
Backing up HA data.	Wait till HA data backup ends.

Reason Why an AP Fails to Go Online	Suggestion
Insufficient LPU resources.	All the resources of the card are occupied. Go online through another card.
Invalid port on the switch connected to the AP.	Check whether a card does not support AP access or the cards are in different working groups.
Insufficient trunk resources.	The trunk resources are released.
The number of distribute APs reaches the upper limit of the central AP.	Re-plan the network and expand the network capacity by adding central APs.
The number of CAPWAP tunnels reaches the upper limit.	Run the **display as** command to check whether any online AS occupies CAPWAP resources. If so, properly allocate CAPWAP resources.
This AP type is not supported. Add it or upgrade the AC version.	Add the AP type or upgrade the AC version.
Inconsistent type IDs on the AP and AC. (Type ID reported by the AP: *xx*; AP type: *yy*)	Modify the AP type ID to be the same as that on the AC. The method is as follows: 1. Run the **undo ap** { **ap-name** *ap-name* | **ap-id** *ap-list* | **ap-mac** *ap-mac* } command to delete all the APs using this type ID. 2. Run the **undo ap-type** *type-description* command to delete the AP type configuration. 3. Run the **ap-type** *type-description* **type-id** *type-id* command to configure the AP type correctly.
The AC version is not supported by the AP.	Upgrade the AC version.
Failed to add the reported AP type parameters.	Upgrade the AC version.
The AP is forcibly disconnected.	iMaster NCE-Campus responds with a registration failure message. In this case, add the AP on iMaster NCE-Campus.
This AP type is not supported.	Replace the AP.

Reason Why an AP Fails to Go Online	Suggestion
DTLS negotiation failed by using the preset certificate.	The function of verifying the CN field in AC certificates is configured on the AP. In an AC replacement scenario, if the CN field of the new AC is not added, APs cannot go online on the new AC. In this case, you need to add the CN field of the new AC for APs on the original AC. If the original AC is faulty and does not support the configuration, log in to each AP that fails to go online and run the **capwap dtls server-auth disable** command to disable the AC authentication function for the AP or restore the factory settings of each AP.
The AP automatic replacement function is enabled, and the AP does not carry LLDP neighbor information.	Check whether LLDP is enabled on the device connected to the AP's uplink interface.
Cloud licenses expire, and local license resources are insufficient	Expand the license capacity. (RUs do not consume license resources.)
Incompatible DTLS version or encryption algorithm	Upgrade the AP version, or run the **capwap dtls version1.0 enable** and **capwap dtls cbc enable** commands to enable compatibility with earlier DTLS versions.
Negotiation DTLS data tunnel failed	Check whether the PSK used for DTLS encryption is correctly configured.
Access through VPN is rejected	The AP cannot go online through a VPN. Ensure that no VPN configuration exists on the interface connecting the upstream device to the AP.
The radio type is inconsistent between the AC and AP	No action is required. The AP automatically restarts and the new configuration takes effect.
The total number of APs and tunnel APs reaches the maximum number of APs that can be managed	Run the **display ap all** and **display tunnel-ap all** commands to check the number of APs and the number of tunnel APs, respectively. Plan APs properly or expand the capacity based on the maximum number of APs that can be managed.

11.1.61 display ap radio-mode all

Function

The **display ap radio-mode all** command displays the effective radio mode of online APs.

Format

display ap radio-mode all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After switching the radio mode of an AP using the **radio-mode** command, you can run the **display ap radio-mode all** command to query the effective radio mode of the AP.

Example

Display the effective radio mode of online APs.

```
<HUAWEI> display ap radio-mode all
-------------------------------------------
ID      Mode
-------------------------------------------
0       2radio-standard
-------------------------------------------
Total: 1
```

Table 11-15 Description of the **display ap radio-mode all** command output

Item	Description
ID	AP ID.

Item	Description
Mode	Radio mode. • 2radio-standard: standard dual-radio mode • 2radio-2g-enhanced: 2G enhanced dual-radio mode • 2radio-5g-enhanced: 5G enhanced dual-radio mode • 2radio-independent-scan: dual-radio + independent scanning mode • 3radio: three-radio mode • -: The AP has not reported the radio mode switching message. **NOTE** The AirEngine 6761-21, AirEngine 6761-21E, and AirEngine 6761S-21 have a dedicated radio for scanning and can perform radio scanning even in **2radio-standard** mode.

11.1.62 display ap-rtu-status all

Function

The **display ap-rtu-status all** command displays the RTU license loading status of all APs.

NOTE

The RTU License is not supported by the following models.

- AirEngine x76x (Excluding the AirEngine 5760-51, AirEngine 6760-X1, AirEngine 6760-X1E)
- AirEngine x77x
- The cemtral AP (including matching RUs)
- AirEngine 9700D-S (including matching ORUs)

Format

display ap-rtu-status all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After loading RTU licenses to APs, you can run this command to check the RTU license loading status.

Precautions

If the number of RTU licenses exceeds the maximum number of RTU licenses supported by an AC, the excess RTU licenses cannot be displayed in the command output. To check information about these RTU licenses, run the **dir rtu/** command in the user view.

Example

Display the RTU license loading status of all APs.

```
<HUAWEI> display ap-rtu-status all
Info: This operation may take a few seconds. Please wait for a moment.done.
Active: [1] The RTU license is activated on the AP.
Activating(Init):[1] The AC has not delivered the RTU file to the AP.
Activating(Need reboot): [1] The AP has downloaded the RTU license and needs a restart for the license to take effect.
Active fail(Flash memory not enough): [1] The flash memory on the AP is insufficient for storing the license file. Manually clear the flash space on the AP.
Active fail(Invalid license): [1] Invalid license file. Verify that the license file is correct.
No RTU license: [1] The license file of the AP does not exist on the AC. Upload the RTU package available for this AP and run the ap rtu load command to decompress the package.
Not support RTU:[2] The AP version or model does not support the RTU license.
Not active:[3] The RTU license on the AC does not have the corresponding AP.
--------------------------------------------------------------
AP ID  AP name    RTU license SN            RTU status
--------------------------------------------------------------
1      AP-1       2102351TYRW0KB001030      Active
2      AP-2       2102353KCN10L1000053      Activating(Need reboot)
3      AP-3       2102353GSF10KC00002       No license on AP
4      AP-4       -                         No RTU license
5      AP-5       2102353GSF10KC00003       Active fail(Flash memory not enough)
6      AP-6       2102353GSF10KC00004       Active fail(Invalid license)
7      AP-7       2102353GSF10KC00005       Not support RTU
8      AP-8       -                         Not support RTU
9      AP-9       2102353GSF10KC00006       Activating(Init)
-      -          2102353GSF10KC10005       Not active
-      -          2102353GSF10KC20005       Not active
-      -          2102353GSF10KC30005       Not active
--------------------------------------------------------------
Total: 12
```

Table 11-16 Description of the **display ap-rtu-status all** command output

Item	Description
AP ID	AP ID.
AP name	AP name.

Item	Description
RTU license SN	ESN in the RTU license file, which is not the ESN of the AP. If no ESN or an invalid ESN is contained in a license file, the file is considered invalid and this field is displayed as -. If the license file does not contain the RTU license file for the AP, this field is displayed as -.
RTU status	RTU license loading status. ● Active: The RTU license has been activated on an AP. ● Activating(Init): The AC has not delivered the RTU license file to an AP. ● Activating(Need reboot): An AP has downloaded and stored the RTU license file, and needs a restart for the file to take effect. ● No RTU license: The AC does not have the RTU license file for an AP. You need to upload the RTU license package containing the RTU license for the AP and run the **ap rtu load** command to unzip the package. ● Active fail(Flash memory not enough): The flash memory on an AP has insufficient space to store the RTU license file. You need to manually clear the flash memory on the AP. ● Active fail(Invalid license): The RTU license file is invalid. Verify that the file is correct. ● Not support RTU: The model software version or model of an AP does not support the RTU license. ● Not active: The AC has the RTU license but the corresponding AP is not online on the AC. ● -: An AP goes online on the standby AC. Query the RTU license on the active AC.

11.1.63 display ap sta-signal strength

Function

The **display ap sta-signal strength** command displays the average signal strength of STAs connected to an AP.

Format

display ap sta-signal strength { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the average signal strength of STAs connected to the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the average signal strength of STAs connected to the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Displays the average signal strength of STAs connected to a specified AP radio.	The radio ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the average signal strength of STAs connected to an AP.

Example

Display the average signal strength of STAs connected to AP **test**.

```
<HUAWEI> display ap sta-signal strength ap-name test
Station signal strength(dBm): 0
```

Table 11-17 Description of the **display ap sta-signal strength** command output

Item	Description
Station signal strength(dBm)	Average signal strength of STAs.

11.1.64 display ap statistics

Function

The **display ap statistics** command displays AP type statistics.

Format

display ap statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Various types of APs can be added on the device. You can run this command to view types of APs added on the device and the number of APs of various types.

Example

Display statistics about AP types.

```
<HUAWEI> display ap statistics
--------------------------------------------------------------------------------
Type                    Number
--------------------------------------------------------------------------------
AP4050DN                1
AP5030DN                1
--------------------------------------------------------------------------------
```

Table 11-18 Description of the **display ap statistics** command output

Item	Description
Type	AP type.
Number	Number of APs of a type.

11.1.65 display ap unauthorized record

Function

The **display ap unauthorized record** command displays information about unauthenticated APs.

Format

display ap unauthorized record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the MAC address or SN authentication mode is configured for an AP but the AP is neither imported nor added to the whitelist, the AC does not allow this AP to access. You can run the **display ap unauthorized record** command to view information about unauthorized APs.

Example

Display information about unauthorized APs.

```
<HUAWEI> display ap unauthorized record
Unauthorized AP record:
Total number: 1
------------------------------------------------------------------------------
AP type: AirEngine8760-X1-PRO
AP SN: xxxxxxxxxxxxxxxx
AP MAC address: xxxx-xxxx-xxxx
AP IP address: 192.168.109.252
Record time: 2020-01-22 17:23:17
------------------------------------------------------------------------------
```

Table 11-19 Description of the **display ap unauthorized record** command output

Item	Description
Unauthorized AP record	Records about unauthenticated APs.
Total number	Total number of unauthenticated APs.
AP type	AP type.
AP SN	AP SN.
AP MAC address	AP's MAC address.
AP IP address	AP's IP address.
Record time	Time when an unauthorized AP was recorded.

11.1.66 display ap whitelist

Function

The **display ap whitelist** command displays AP whitelist information.

Format

display ap whitelist { **mac** | **sn** }

Parameters

Parameter	Description	Value
sn	Displays SNs in the AP whitelist.	-
mac	Displays MAC addresses in the AP whitelist.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the AP authentication mode is set to MAC address or SN authentication using the **ap auth-mode** command, you can run the **ap whitelist** command to configure an AP whitelist. Only RUs on the whitelist are allowed to go online. To check information about RUs in the whitelist, run the **display ap whitelist** command.

Example

Display MAC addresses in the AP whitelist.

```
<HUAWEI> display ap whitelist mac
--------------------------------------------------------------------------------
Index  MAC
--------------------------------------------------------------------------------
0      00e0-fcb1-56a0
1      00e0-fc24-0080
2      00e0-fc9d-0bb0
--------------------------------------------------------------------------------
Total: 3
```

Table 11-20 Description of the **display ap whitelist mac** command output

Item	Description
Index	Index.
MAC	MAC address of an AP. To add a MAC address to the AP whitelist, run the **ap whitelist mac** *ap-mac1* [**to** *ap-mac2*] command.

Display SNs in the AP whitelist.

```
<HUAWEI> display ap whitelist sn
--------------------------------------------------------------------------------
Index  SN
--------------------------------------------------------------------------------
0      210235449210CB000011
1      S0001
2      210235568010D1000032
--------------------------------------------------------------------------------
Total: 3
```

Table 11-21 Description of the **display ap whitelist sn** command output

Item	Description
Index	Index.
SN	SN of an AP. To add an SN to the AP whitelist, run the **ap whitelist sn** *ap-sn1* [**to** *ap-sn2*] command.

11.1.67 display ap-group

Function

The **display ap-group** command displays configuration and reference information about an AP groups.

Format

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

Parameters

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

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap-group** command to view configuration and reference information about AP groups.

Example

Display information about all AP groups.

```
<HUAWEI> display ap-group all
------------------------------------------------------------
Name                          APs
------------------------------------------------------------
default                       1
------------------------------------------------------------
Total: 1
```

Table 11-22 Description of the **display ap-group all** command output

Item	Description
Name	Name of an AP group.
APs	Number of APs in an AP group.

Display information about the AP group **default**.

```
<HUAWEI> display ap-group name default
------------------------------------------------------------------------------------------
AP system profile          : default
Regulatory domain profile  : default
WIDS profile               : default
BLE profile                :
AP location                :
UUID                       :
Domain name                :
Scene                      : multi-partition-cross-room
Ap pki profile             :
AP wired port profile
 Interface FE0             : default
 Interface FE1             : default
 Interface FE2             : default
 Interface FE3             : default
 Interface GE0             : default
......
 Interface GE27            : default
 Interface MultiGE0        : default
......
 Interface MultiGE7        : default
 Interface XGE0            : default
......
 Interface XGE7            : default
 Interface Eth-trunk0      : default
 Interface Eth-trunk1      : default
Radio 0
 Radio 2.4G profile        : default
 Radio 5G profile          : default
 VAP profile               :
 Mesh profile              :
 WDS profile               :
 Mesh whitelist profile    :
 WDS whitelist profile     :
 Location profile          :
```



```
 Radio switch              : enable
 Channel                 : -
 Channel bandwidth         : 20mhz
 EIRP(dBm)               : 127
 Antenna gain(dB)          : -
 Coverage distance(100 m)  : 3
 Work mode               : normal
 Flexible radio switch     : on
 Radio frequency           : 2.4G
 Spectrum analysis         : disable
 Channel monitor           : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
 Auto channel select       : enable
 Auto bandwidth select     : disable
 Auto transmit power select: enable
 Reference data-analysis   : enable
 Reference 3d-data         : enable
 Beacon switch             : enable
 CTS switch              : enable
 CTS delay time(us)        : none
Radio 1
......
Radio 2
......
Card 1
 Card connect type         : -
 Baud rate               : -
 Wired port profile        : default
 Iot profile             :
 Protocol Type           : -
 First Port              : -
 Extended Port           : -
Card 2
......
Card usb
 Card connect type         : -
 Baud rate               : -
 Wired port profile        : default
 Iot profile             :
 Protocol Type           : -
 First Port              : -
 Extended Port           : -
Traffic policy outbound    : 1
```

Table 11-23 Description of the **display ap-group name** command output

Item	Description
AP system profile	AP system profile referenced by an AP group. To configure this parameter, run the **ap-system-profile (AP group view and AP view)** command.
Regulatory domain profile	Regulatory domain profile referenced by an AP group. To configure this parameter, run the **regulatory-domain-profile** command.
WIDS profile	WIDS profile referenced by an AP group.

Item	Description
BLE profile	BLE profile referenced by an AP group. To configure this parameter, run the **ble-profile (AP group view and AP view)** command.
UUID	UUID of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP group view)** command.
AP location	Installation position of an AP in the AP group. To configure this parameter, run the **location** command.
Domain name	Default domain name suffix of the AP. To configure this parameter, run the **ip domain-name** command.
Scene	Scenario profile bound to an AP group. To configure this parameter, run the **scene** command.
Ap pki profile	Bound AP PKI realm profile. To configure this parameter, run the **ap-pki-profile** command.
AP wired port profile	AP wired port profile referenced by an AP group. To configure this parameter, run the **wired-port-profile (AP group view and AP view)** command.
Interface *Interface-name*	Interface name.
Radio 0/Radio 1/Radio 2	Radio ID.
Radio 2.4G profile	2G radio profile referenced by an AP group. To configure this parameter, run the **radio-2g-profile** command.
Radio 5G profile	5G radio profile referenced by an AP group. To configure this parameter, run the **radio-5g-profile** command.

Item	Description
VAP profile	VAP profile referenced by an AP group. The displayed format is "VAP ID:VAP profile name (service VLAN defined when binding to the VAP profile, single VLAN, or VLAN pool)." To configure this parameter, run the **vap-profile** command.
Mesh profile	Mesh profile referenced by an AP group. To configure this parameter, run the **mesh-profile radio** command.
WDS profile	WDS profile referenced by an AP group. To configure this parameter, run the **wds-profile radio** command.
Mesh whitelist profile	Mesh whitelist profile referenced by an AP group. To configure this parameter, run the **mesh-whitelist-profile (AP group radio view or AP radio view)** command.
WDS whitelist profile	WDS whitelist profile referenced by an AP group. To configure this parameter, run the **wds-whitelist-profile (AP group radio view or AP radio view)** command.
Location profile	Location profile referenced by an AP group. To configure this parameter, run the **location-profile** command.
Radio switch	Whether a radio is enabled. To configure this parameter, run the **radio disable** command.
Channel	Working channel of a radio. To configure this parameter, run the **channel** command.
Channel bandwidth	Working bandwidth of a radio. To configure this parameter, run the **channel** command.

Item	Description
EIRP(dBm)	Transmit power of a radio, in dBm. To configure this parameter, run the **eirp** command.
Antenna gain(dB)	Antenna gain of a radio, in dB. To configure this parameter, run the **antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter, in the unit of 100 m. To configure this parameter, run the **coverage distance** command.
Work mode	Working mode of a radio. To configure this parameter, run the **work-mode** command.
Flexible radio switch	Whether the DFA function of a radio is enabled. To configure this parameter, run the **calibrate flexible-radio disable** command.
Radio frequency	Working frequency band of a radio. To configure this parameter, run the **frequency** command.
Spectrum analysis	Whether spectrum analysis is enabled. To configure this parameter, run the **spectrum-analysis enable** command.
Channel monitor	Whether the function of monitoring the status of all channels is enabled. To configure this parameter, run the **channel-monitor enable** command.
WIDS device detect	Whether wireless device detection is enabled. To configure this parameter, run the **wids device detect enable** command.
WIDS attack detect	Whether attack detection is enabled. To configure this parameter, run the **wids attack detect** command.
WIDS contain switch	Whether rogue device containment is enabled. To configure this parameter, run the **wids contain enable** command.

Item	Description
Auto channel select	Whether automatic channel selection is enabled. To configure this parameter, run the **calibrate auto-channel-select** command.
Auto bandwidth select	Whether automatic bandwidth selection is enabled. To configure this parameter, run the **calibrate auto-bandwidth-select** command.
Auto transmit power select	Whether automatic transmit power selection is enabled. To configure this parameter, run the **calibrate auto-txpower-select** command.
Reference data-analysis	Whether big data calibration is enabled. To configure this parameter, run the **calibrate reference data-analysis { disable | enable }** command.
Reference 3d-data	Whether 3D radio calibration is enabled. To configure this parameter, run the **calibrate reference 3d-data { disable | enable }** command.
Beacon switch	Whether RUs are enabled to send Beacon frames. To configure this parameter, run the **beacon disable** command.
CTS switch	Whether RUs are enabled to respond to STAs with CTS packets. To configure this parameter, run the **cts disable** command.
CTS delay time(us)	Delay time after which RUs respond to STAs with CTS packets. To configure this parameter, run the **cts delay** command.
Card 1/Card 2/Card 3/Card usb	IoT card.

Item	Description
Card connect type	Communication connection type between IoT cards and APs. To configure this parameter, run the **card connect-type** command.
Baud rate	Baud rate used for communication between an IoT card and the AP. To configure this parameter, run the **baud-rate** command.
Wired port profile	AP wired port profile referenced by an AP group. To configure this parameter, run the **wired-port-profile (IoT card interface view)** command.
Iot profile	Bound IoT profile. To configure this parameter, run the **iot-profile (IoT card interface view)** command.
Protocol Type	Communication protocol between the AP and host computer.
First Port	Source port for the first channel.
Extended Port	Source port for the extended channel.
Traffic policy outbound	Traffic policy applied to an AP group.

11.1.68 display capwap configuration

Function

The **display capwap configuration** command displays the CAPWAP configuration.

Format

display capwap configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the interval for sending Keepalive packets, number of times for sending Keepalive packets, and priority of CAPWAP management packets.

Example

Display the CAPWAP configuration.

```
<HUAWEI> display capwap configuration
  ------------------------------------------------------------------
  Source interface                          : -
  Echo interval(seconds)                    : 25
  Echo times                                : 6
  Control priority(server to client)        : 7
  Control priority(client to server)        : 7
  Control-link DTLS encrypt                 : disable
  DTLS PSK value                            : ******
  Control-link inter-controller DTLS encrypt      : disable
  Inter-controller DTLS PSK value           : ******
  Message-integrity PSK value               : ******
  Message-integrity check switch            : enable
  Sensitive-info PSK value                  : ******
  Sensitive-info inter-controller PSK value       : ******
  DTLS no-auth status                       : disable
  DTLS cert-mandatory-match status          : disable
  DTLS version1.0 status                    : disable
  DTLS cbc status                           : disable
  ------------------------------------------------------------------
```

Table 11-24 Description of the **display capwap configuration** command output

Item	Description
Source interface	Source interface of the AC. To configure this parameter, run the **capwap source interface** command.
Echo interval(seconds)	Interval for sending Keepalive packets. To configure this parameter, run the **capwap echo interval** *interval-value* command.
Echo times	Number of times for sending Keepalive packets. If no response is received after the specified number of times, the link is considered disconnected. To configure this parameter, run the **capwap echo times** *times-value* command.

Item	Description
Control priority(server to client)	Priority of CAPWAP management packets from the AC to the APs. To configure this parameter, run the **capwap control-link-priority local** *priority-value* command.
Control priority(client to server)	Priority of CAPWAP management packets from the APs to the AC. To configure this parameter, run the **capwap control-link-priority remote** *priority-value* command.
Control-link DTLS encrypt	Whether DTLS encryption for CAPWAP control tunnels is enabled. To configure this parameter, run the **capwap dtls control-link encrypt** command.
DTLS PSK value	PSK for DTLS encryption. To configure this parameter, run the **capwap dtls psk** command.
Control-link inter-controller DTLS encrypt	Whether DTLS encryption is enabled for control tunnels between ACs. To configure this parameter, run the **capwap dtls inter-controller control-link encrypt** command.
Inter-controller DTLS PSK value	PSK for DTLS encryption of an inter-AC tunnel. To configure this parameter, run the **capwap dtls inter-controller psk** command.
Message-integrity PSK value	PSK for checking integrity of CAPWAP packets. To configure this parameter, run the **capwap message-integrity psk** command.
Message-integrity check switch	Whether integrity check of CAPWAP packets is enabled. To configure this parameter, run the **capwap message-integrity check disable** command.
Sensitive-info PSK value	PSK for encrypting sensitive information. To configure this parameter, run the **capwap sensitive-info psk** command.

Item	Description
Sensitive-info inter-controller PSK value	PSK for encrypting sensitive information between ACs. To configure this parameter, run the **capwap inter-controller sensitive-info psk** command.
DTLS no-auth status	Whether the function of establishing CAPWAP DTLS sessions in none authentication mode is enabled. To configure this parameter, run the **capwap dtls no-auth enable** command.
DTLS cert-mandatory-match status	Whether the function of establishing CAPWAP DTLS sessions through the initial certificate is enabled. To configure this parameter, run the **capwap dtls cert-mandatory-match disable** command.
DTLS version1.0 status	Whether compatibility with DTLS 1.0 is enabled. To configure this parameter, run the **capwap dtls version1.0 enable** command.
DTLS CBC status	Whether compatibility with the DTLS CBC cipher suite is enabled. To configure this parameter, run the **capwap dtls cbc enable** command.

11.1.69 display cpe-tunnel-profile

Function

The **display cpe-tunnel-profile** command displays configuration and reference information about CPE tunnel profiles.

Format

display cpe-tunnel-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all CPE tunnel profiles.	-
name *profile-name*	Displays information about a specified CPE tunnel profile.	The CPE tunnel profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check configuration and reference information about CPE tunnel profiles.

Example

Display information about all CPE tunnel profiles.

```
<HUAWEI> display cpe-tunnel-profile all
-------------------------------------------------------------------------------------------------------
Profile name          Reference
-------------------------------------------------------------------------------------------------------
default               1
cpe-tunnel-profile1   0
-------------------------------------------------------------------------------------------------------
Total: 2
```

Table 11-25 Description of the **display cpe-tunnel all** command output

Item	Description
Profile name	Name of a CPE tunnel profile.
Reference	Number of times a CPE tunnel profile is referenced.

Display information about the CPE tunnel profile **cpe1**.

```
<HUAWEI> display cpe-tunnel-profile name cpe1
-------------------------------------------------------------------------
PVID VLAN                          : 100
GRE checksum                       : disable
GRE key                            : disable
Allow-pass VLAN                    : 1 100
Forward mode                       : tunnel
Wlan-slice high-reliability traffic filter info:
```



```
AppliedRecord:
--------------------------------------------------------------------------------
```

Table 11-26 Description of the **display cpe-tunnel-profile name** command output

Item	Description
PVID VLAN	PVID of the interface corresponding to the CPE tunnel.
GRE checksum	Whether the checksum function is enabled for the CPE tunnel. To configure this parameter, run the **gre checksum (CPE tunnel profile view)** command.
GRE key	GRE key status of the CPE tunnel. To configure this parameter, run the **gre key (CPE tunnel profile view)** command.
Allow-pass VLAN	VLANs from which packets are allowed to pass through the CPE tunnel.
Forward mode	Forwarding mode of the CPE tunnel. • direct-forward: direct forwarding • tunnel: tunnel forwarding To configure this parameter, run the **forward-mode (CPE tunnel profile view)** command.
AppliedRecord(Wlan-slice high-reliability traffic filter info)	ACL-based rule records for air interface slicing. To configure this parameter, run the **wlan-slice high-reliability acl** command.

11.1.70 display radio

Function

The **display radio** command displays AP radio information.

Format

display radio { **all** | **ap-group** *ap-group-name* | **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Displays radio information about all APs.	-
ap-group *ap-group-name*	Displays radio information about all APs in a specified AP group.	The AP group must exist.
ap-name *ap-name*	Displays radio information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays radio information about the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the working status of AP radios.

Example

Display radio information about all APs.

```
<HUAWEI> display radio all
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
WM:Working Mode (normal/monitor/monitor dual-band-scan/monitor proxy dual-band-scan)
--------------------------------------------------------------------------------
 AP ID Name           RfID  Band  Type    ST  CH/BW    CE/ME   STA     CU    WM
--------------------------------------------------------------------------------
 0     00e0-fc76-e360 0     2.4G  bgn     on  6/20M    24/24   0       55%   normal
 0     00e0-fc76-e360 1     5G    an      on  56/20M   25/25   0       3%    normal
--------------------------------------------------------------------------------
Total:2
```

Table 11-27 Description of the **display radio** command output

Item	Description
AP ID	AP ID.
Name	AP name.
RfID	Radio ID.

Item	Description
Band	Operating frequency band of an AP radio.
Type	Protocol type of an AP radio. • b: 802.11b radio type • bg: 802.11b/g radio type • bgn: 802.11b/g/n radio type • a: 802.11a radio type • an: 802.11a/n radio type • an11ac: 802.11a/n/ac radio type • 11ax: 802.11b/g/n/ax radio type for a 2.4 GHz radio; 802.11a/n/ac/ax radio type for a 5 GHz radio; or 802.11ax radio type for a 6 GHz radio • 11be: 802.11b/g/n/ax/be radio type for a 2.4 GHz radio; 802.11a/n/ac/ax/be radio type for a 5 GHz radio; or 802.11ax/be radio type for a 6 GHz radio
ST	Working status of an AP radio.
CH/BW	Channel/Bandwidth of an AP radio. If no VAP profile is bound to the radio, a hyphen (-) is displayed.
CE/ME	Current transmit power of an AP radio/ Maximum transmit power of an AP radio. If no VAP profile is bound to the radio, a hyphen (-) is displayed. **NOTE** The value is calculated based on the typical gain of the antenna used by the AP.
STA	Number of STAs connected to an AP radio.

Item	Description
CU	Channel utilization. When an AP radio works in monitor mode, this parameter is displayed as **-**. ● In the AC+central AP+RU networking: RUs do not proactively report the channel utilization to the AC. To query the channel utilization of RUs, enable the data buffer function on the AC. **NOTE** The **ap data-collection enable** command enables the data buffer function on the AC. After this command is executed, a large data buffer occupies the device memory and affects device performance. It is recommended that the **undo ap data-collection enable** command be executed to disable data buffer after the query. ● In the AC+Fit AP networking: A Fit AP periodically reports the channel utilization to the AC. Therefore, the AC does not need to query the channel utilization of APs.
WM	Working mode of an AP radio. ● normal ● monitor ● monitor dual-band-scan: inter-band scanning mode ● monitor proxy dual-band-scan: proxy inter-band scanning mode

11.1.71 display radio-2g-profile

Function

The **display radio-2g-profile** command displays configuration and reference information about a 2G radio profile.

Format

display radio-2g-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all 2G radio profiles.	-
name *profile-name*	Displays information about a specified 2G radio profile.	The 2G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about a 2G radio profile.

Example

Display information about all 2G radio profiles.

```
<HUAWEI> display radio-2g-profile all
------------------------------------------------------------------
Profile name  Config Reference  Reference radios
------------------------------------------------------------------
default       10               4
------------------------------------------------------------------
Total: 1
```

Table 11-28 Description of the **display radio-2g-profile all** command output

Item	Description
Profile name	Name of a 2G radio profile.
Config Reference	Number of times a 2G radio profile is referenced.
Reference radios	Number of radios that reference a 2G radio profile.

Display information of the 2G radio profile **default**.

```
<HUAWEI> display radio-2g-profile name default
------------------------------------------------------------
Radio type                      : 802.11n
```



```
Power auto adjust                    : disable
Beacon interval(TUs)                 : 100
Beamforming switch                   : disable
Support short preamble               : support
Fragmentation threshold(Byte)        : 2346
Channel switch announcement          : enable
Channel switch mode                  : continue
Guard interval mode                  : normal
802.11ax Guard interval mode         : dot8
A-MPDU switch                        : enable
HT A-MPDU length limit               : 3
A-MSDU switch                        : disable
RTS-CTS-mode                         : cts-to-self
RTS-CTS-threshold                    : 2347
802.11bg basic rate                  : 1 2
802.11bg support rate                : 1 2 5 6 9 11 12 18 24 36 48 54
Multicast rate 2.4G                  : 11
Interference detect switch           : disable
Co-channel frequency interference threshold(%)        : 50
Adjacent-channel frequency interference threshold(%)  : 50
Station interference threshold       : 32
WMM switch                           : enable
Mandatory switch                     : disable
Auto-off start time                  : -
Auto-off end time                    : -
Auto-off time-range                  : -
Wifi-light mode                      : signal-strength
Utmost power switch                  : enable
Rrm-profile                          : default
Air-scan-profile                     : default
Smart-antenna                        : disable
Agile-antenna-polarization           : disable
CCA threshold(dBm)                   : -
RX sensitivity(dBm)                  : -128
AGC high threshold(dBm)              : -82
High PER threshold(%)                : 80
Low PER threshold(%)                 : 20
Training interval(s)                 : auto
Training mpdu num                    : 640
Throughput trigger training threshold (%)       : 10
VIP user bandwidth reservation ratio (%)        : 20
Legacy signal length compatible                 : enable
RX STBC                              : enable
Fastpass users                       : 5
Fastpass period(ms)                  : 20
Fastpass ratio(%)                    : 25
Radio reload time-range              : test
------------------------------------------------------------------
AP EDCA parameters:
------------------------------------------------------------------
      ECWmax  ECWmin  AIFSN  TXOPLimit(32us)  Ack-Policy
AC_VO  3       2       1      47              normal
AC_VI  4       3       1      94              normal
AC_BE  6       4       3      0               normal
AC_BK  10      4       7      0               normal
------------------------------------------------------------------
```

Table 11-29 Description of the **display radio-2g-profile name** command output

Item	Description
Radio type	Radio type. To configure this parameter, run the **radio-type (2G radio profile view)** command.

Item	Description
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure this parameter, run the **power auto-adjust enable** command.
Beacon interval(TUs)	Interval at which an AP sends Beacon frames, in TUs. To configure this parameter, run the **beacon-interval** command.
Beamforming switch	Whether the beamforming function is enabled. To configure this parameter, run the **beamforming enable** command. This configuration takes effect only on APs running V200R019C00 or earlier.
Support short preamble	Whether the short preamble is supported. To configure this parameter, run the **short-preamble disable** command.
Fragmentation threshold(Byte)	Packet fragmentation threshold, in bytes. To configure this parameter, run the **fragmentation-threshold** command.
Channel switch announcement	Whether channel switch announcement is enabled. To configure this parameter, run the **channel-switch announcement disable** command.
Channel switch mode	Channel switch announcement mode. To configure this parameter, run the **channel-switch mode** command.
Guard interval mode	802.11n/ac GI mode. To configure this parameter, run the **guard-interval-mode** command.
802.11ax Guard interval mode	802.11ax/be GI mode. ● dot8: 0.8us ● 1dot6: 1.6us ● 3dot2: 3.2us To configure this parameter, run the **guard-interval-mode** command.

Item	Description
A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure this parameter, run the **a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure this parameter, run the **ht a-mpdu max-length-exponent** command.
A-MSDU switch	Whether to enable the function of sending 802.11 packets in A-MSDU mode. To configure this parameter, run the **a-msdu enable** command.
RTS-CTS-mode	RTS/CTS mode. To configure this parameter, run the **rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure this parameter, run the **rts-cts-threshold** command.
802.11bg basic rate	802.11bg basic rate set. To configure this parameter, run the **dot11bg basic-rate** command.
802.11bg support rate	802.11bg supported rate set. To configure this parameter, run the **dot11bg supported-rate** command.
Multicast rate 2.4G	Multicast rate of wireless packets on the 2.4 GHz radio. To configure this parameter, run the **multicast-rate** command.
Interference detect switch	Whether interference detection is enabled. To configure this parameter, run the **interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure this parameter, run the **interference co-channel threshold** command.

Item	Description
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure this parameter, run the **interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure this parameter, run the **interference station threshold** command.
WMM switch	Whether the WMM function is enabled. To configure this parameter, run the **wmm disable** command.
Mandatory switch	Whether to allow STAs that do not support WMM to connect to a WMM-enabled AP. To configure this parameter, run the **wmm mandatory enable** command.
Auto-off start time	Start time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Auto-off end time	End time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Wifi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure this parameter, run the **wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure this parameter, run the **rrm-profile (radio profile view)** command.
Air-scan-profile	Name of the air scan profile referenced by a radio profile. To configure this parameter, run the **air-scan-profile (radio profile view)** command.

Item	Description
Smart-antenna	Status of the smart antenna function. To configure this parameter, run the **smart-antenna { enable | disable }** command.
Agile-antenna-polarization	Status of the self-adaptive polarization for agile antennas. To configure this parameter, run the **agile-antenna-polarization** command.
CCA threshold(dBm)	CCA threshold for APs. To configure this parameter, run the **cca-threshold** command.
RX sensitivity(dBm)	Receiver sensitivity threshold. To configure this parameter, run the **rx-sensitivity** command.
AGC high threshold(dBm)	Upper AGC threshold. To configure this parameter, run the **agc-threshold** command.
High PER threshold(%)	Upper valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **smart-antenna valid-per-scope** command.
Low PER threshold(%)	Lower valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **smart-antenna valid-per-scope** command.
Training interval(s)	Smart antenna training interval. To configure this parameter, run the **smart-antenna training-interval** command.
Training mpdu num	Number of MPDUs sent by an AP to STAs during smart antenna training. To configure this parameter, run the **smart-antenna training-mpdu-number** command.

Item	Description
Throughput trigger training threshold (%)	Sudden performance change threshold that triggers smart antenna training. To configure this parameter, run the **smart-antenna throughput-triggered-training** command.
VIP user bandwidth reservation ratio (%)	Percentage of bandwidth reserved for VIP users. To configure this parameter, run the **vip-user bandwidth reservation-ratio** command.
Legacy signal length compatible	Whether the L-SIG field length compatibility function of the 802.11n protocol is enabled. To configure the parameter, run the **dot11n legacy-signal-length-compatible enable** command.
RX STBC	Whether the STBC encoding function in the receive direction is enabled. To configure this parameter, run the **rx-stbc disable** command.
Fastpass users	Number of FastPass users. This parameter is valid only for DAPs. To configure this parameter, run the **fastpass users** command.
Fastpass period(ms)	FastPass scheduling period. This parameter is valid only for DAPs. To configure this parameter, run the **fastpass users** command.
Fastpass ratio(%)	Percentage of FastPass users in the scheduling period. This parameter is valid only for DAPs. To configure this parameter, run the **fastpass users** command.
Radio reload time-range	Time range during which radios are reloaded as scheduled. To configure this parameter, run the **radio-reload time-range** command.
Utmost power switch	Whether a radio is enabled to send packets at maximum power. To configure this parameter, run the **utmost-power** command.

Item	Description
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure this parameter, run the **wmm edca-ap** command.
AC_VO	AC_VO packets. To configure this parameter, run the **wmm edca-ap** command.
AC_VI	AC_VI packets. To configure this parameter, run the **wmm edca-ap** command.
AC_BE	AC_BE packets. To configure this parameter, run the **wmm edca-ap** command.
AC_BK	AC_BK packets. To configure this parameter, run the **wmm edca-ap** command.
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **wmm edca-ap** command.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure this parameter, run the **wmm edca-ap** command.
TXOPLimit(32us)	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger value indicates a longer duration. To configure this parameter, run the **wmm edca-ap** command.

Item	Description
Ack-Policy	ACK policy. It includes: • **normal**: During 802.11 packet exchange, the receiver sends an ACK packet to confirm the receiving of a packet from the sender. • **noack**: The receiver sends no ACK packet to confirm the receiving of a packet from the sender. It applies to scenarios where communication quality is good and interference is low. To configure this parameter, run the **wmm edca-ap** command.

11.1.72 display radio-5g-profile

Function

The **display radio-5g-profile** command displays configuration and reference information about a 5G radio profile.

Format

display radio-5g-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all 5G radio profiles.	-
name *profile-name*	Displays information about a specified 5G radio profile.	The 5G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about a 5G radio profile.

Example

Display information about all 5G radio profiles.

```
<HUAWEI> display radio-5g-profile all
------------------------------------------------------------------------
Profile name  Config Reference  Reference radios
------------------------------------------------------------------------
default       10               4
------------------------------------------------------------------------
Total: 1
```

Table 11-30 Description of the **display radio-5g-profile all** command output

Item	Description
Profile name	Name of a 5G radio profile.
Config Reference	Number of times a 5G radio profile is referenced.
Reference radios	Number of radios that reference a 5G radio profile.

Display information of the 5G radio profile **default**.

```
<HUAWEI> display radio-5g-profile name default
------------------------------------------------------------
Radio type                          : 802.11ac
Power auto adjust                   : disable
Beacon interval(TUs)                : 100
Beamforming switch                  : disable
Fragmentation threshold(Byte)       : 2346
Channel switch announcement         : enable
Channel switch mode                 : continue
Guard interval mode                 : normal
802.11ax guard interval mode        : dot8
A-MPDU switch                       : enable
HT A-MPDU length limit              : 3
VHT A-MPDU length limit             : 7
A-MSDU switch                       : disable
VHT A-MSDU Max frame number         : 2
RTS-CTS-mode                        : RTS-CTS
RTS-CTS-threshold                   : 2347
802.11a basic rate                  : 6 12 24
802.11a support rate                : 6 9 12 18 24 36 48 54
Multicast rate 5G                   : 6
VHT mcs                             : 9 9 9 9 9 9 9 9
Interference detect switch          : disable
Co-channel frequency interference threshold(%)      : 50
Adjacent-channel frequency interference threshold(%)  : 50
Station interference threshold      :32
WMM switch                          : enable
Mandatory switch                    : disable
Auto-off start time                 : -
Auto-off end time                   : -
WiFi-light mode                     : signal-strength
```



```
Utmost power switch                    : enable
Rrm-profile                          : default
Air-scan-profile                      : default
Smart-antenna                          : disable
Agile-antenna-polarization             : disable
CCA threshold(dBm)                     : -
RX sensitivity(dBm)                  : -128
AGC high threshold(dBm)                : -82
High PER threshold(%)                        : 80
Low PER threshold(%)                         : 20
Training interval(s)                    : auto
Training mpdu num                            : 640
Throughput trigger training threshold (%)       : 10
VIP user bandwidth reservation ratio (%)        : 20
Legacy signal length compatible                 : enable
RX STBC                                       : enable
Radio reload time-range                       : test
DFS radar-filter sensitivity                   : 4
---------------------------------------------------------------
AP EDCA parameters:
---------------------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit(32us)  Ack-Policy
AC_VO  3       2       1      47               normal
AC_VI  4       3       1      94               normal
AC_BE  6       4       3      0                normal
AC_BK  10      4       7      0                normal
---------------------------------------------------------------
```

Table 11-31 Description of the **display radio-5g-profile name** command output

Item	Description
Radio type	Radio type. To configure this parameter, run the **radio-type (5G radio profile view)** command.
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure this parameter, run the **power auto-adjust enable** command.
Beacon interval(TUs)	Interval at which an AP sends Beacon frames, in TUs. To configure this parameter, run the **beacon-interval** command.
Beamforming switch	Whether the beamforming function is enabled. To configure this parameter, run the **beamforming enable** command. This configuration takes effect only on APs running V200R019C00 or earlier.
Fragmentation threshold(Byte)	Packet fragmentation threshold, in bytes. To configure this parameter, run the **fragmentation-threshold** command.

Item	Description
Channel switch announcement	Whether channel switch announcement is enabled. To configure this parameter, run the **channel-switch announcement disable** command.
Channel switch mode	Channel switch announcement mode. To configure this parameter, run the **channel-switch mode** command.
Guard interval mode	802.11n/ac GI mode. To configure this parameter, run the **guard-interval-mode** command.
802.11ax guard interval mode	802.11ax/be GI mode. • dot8: 0.8us • 1dot6: 1.6us • 3dot2: 3.2us To configure this parameter, run the **guard-interval-mode** command.
A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure this parameter, run the **a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure this parameter, run the **ht a-mpdu max-length-exponent** command.
VHT A-MPDU length limit	Maximum length of the frame aggregated in A-MPDU mode. To configure this parameter, run the **vht a-mpdu max-length-exponent** command.
A-MSDU switch	Whether to enable the function of sending 802.11 packets in A-MSDU mode. To configure this parameter, run the **a-msdu enable** command.
VHT A-MSDU Max frame number	Maximum number of subframes that can be aggregated into an A-MSDU. To configure this parameter, run the **vht a-msdu max-frame-num** command.

Item	Description
RTS-CTS-mode	RTS/CTS mode. To configure this parameter, run the **rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure this parameter, run the **rts-cts-threshold** command.
802.11a basic rate	802.11a basic rate set. To configure this parameter, run the **dot11a basic-rate** command.
802.11a support rate	802.11a supported rate set. To configure this parameter, run the **dot11a supported-rate** command.
Multicast rate 5G	Multicast rate of wireless packets on the 5 GHz radio. To configure this parameter, run the **multicast-rate** command.
VHT mcs	Maximum MCS value corresponding to a specific number of 802.11ac spatial streams. To configure this parameter, run the **vht mcs-map** command.
Interference detect switch	Whether interference detection is enabled. To configure this parameter, run the **interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure this parameter, run the **interference co-channel threshold** command.
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure this parameter, run the **interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure this parameter, run the **interference station threshold** command.

Item	Description
WMM switch	Whether the WMM function is enabled. To configure this parameter, run the **wmm disable** command.
Mandatory switch	Whether to allow STAs that do not support WMM to connect to a WMM-enabled AP. To configure this parameter, run the **wmm mandatory enable** command.
Auto-off start time	Start time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Auto-off end time	End time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
WiFi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure this parameter, run the **wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure this parameter, run the **rrm-profile (radio profile view)** command.
Air-scan-profile	Name of the air scan profile referenced by a radio profile. To configure this parameter, run the **air-scan-profile (radio profile view)** command.
Utmost power switch	Whether a radio is enabled to send packets at maximum power. To configure this parameter, run the **utmost-power** command.
Smart-antenna	Status of the smart antenna function. To configure this parameter, run the **smart-antenna { enable | disable }** command.

Item	Description
Agile-antenna-polarization	Status of the self-adaptive polarization for agile antennas. To configure this parameter, run the **agile-antenna-polarization** command.
CCA threshold(dBm)	CCA threshold for APs. To configure this parameter, run the **cca-threshold** command.
RX sensitivity(dBm)	Receiver sensitivity threshold. To configure this parameter, run the **rx-sensitivity** command.
AGC high threshold(dBm)	Upper AGC threshold. To configure this parameter, run the **agc-threshold** command.
High PER threshold(%)	Upper valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **smart-antenna valid-per-scope** command.
Low PER threshold(%)	Lower valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **smart-antenna valid-per-scope** command.
Training interval(s)	Smart antenna training interval. To configure this parameter, run the **smart-antenna training-interval** command.
Training mpdu num	Number of MPDUs sent by an AP to STAs during smart antenna training. To configure this parameter, run the **smart-antenna training-mpdu-number** command.
Throughput trigger training threshold (%)	Sudden performance change threshold that triggers smart antenna training. To configure this parameter, run the **smart-antenna throughput-triggered-training** command.

Item	Description
VIP user bandwidth reservation ratio (%)	Percentage of bandwidth reserved for VIP users. To configure this parameter, run the **vip-user bandwidth reservation-ratio** command.
Legacy signal length compatible	Whether the L-SIG field length compatibility function of the 802.11n protocol is enabled. To configure the parameter, run the **dot11n legacy-signal-length-compatible enable** command.
RX STBC	Whether the STBC encoding function in the receive direction is enabled. To configure this parameter, run the **rx-stbc disable** command.
Radio reload time-range	Time range during which radios are reloaded as scheduled. To configure this parameter, run the **radio-reload time-range** command.
DFS radar-filter sensitivity	Sensitivity level of correction for false radar detection. To configure this parameter, run the **dfs radar-filter sensitivity** command.
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure this parameter, run the **wmm edca-ap** command.
AC_VO	AC_VO packets. To configure this parameter, run the **wmm edca-ap** command.
AC_VI	AC_VI packets. To configure this parameter, run the **wmm edca-ap** command.
AC_BE	AC_BE packets. To configure this parameter, run the **wmm edca-ap** command.
AC_BK	AC_BK packets. To configure this parameter, run the **wmm edca-ap** command.

Item	Description
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **wmm edca-ap** command.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure this parameter, run the **wmm edca-ap** command.
TXOPLimit(32us)	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger value indicates a longer duration. To configure this parameter, run the **wmm edca-ap** command.
Ack-Policy	ACK policy. It includes: • **normal**: During 802.11 packet exchange, the receiver sends an ACK packet to confirm the receiving of a packet from the sender. • **noack**: The receiver sends no ACK packet to confirm the receiving of a packet from the sender. It applies to scenarios where communication quality is good and interference is low. To configure this parameter, run the **wmm edca-ap** command.

11.1.73 display references radio-2g-profile

Function

The **display references radio-2g-profile** command displays reference information about a 2G radio profile.

Format

display references radio-2g-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified 2G radio profile.	The 2G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references radio-2g-profile** command to view reference information about a 2G radio profile.

Example

Display reference information about the 2G radio profile **default**.

```
<HUAWEI> display references radio-2g-profile name default
------------------------------------------------------------------------
Reference type  Reference name                  Reference radio
------------------------------------------------------------------------
AP-group        ap-group1                       Radio-0
------------------------------------------------------------------------
Total:1
```

Table 11-32 Description of the **display references radio-2g-profile** command output

Item	Description
Reference type	Type of the profile by which a 2G radio profile is referenced.
Reference name	Name of the profile by which a 2G radio profile is referenced.
Reference radio	Radio to which a 2G radio profile is referenced.

11.1.74 display references radio-5g-profile

Function

The **display references radio-5g-profile** command displays reference information about a 5G radio profile.

Format

display references radio-5g-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified 5G radio profile.	The 5G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references radio-5g-profile** command to view reference information about a 5G radio profile.

Example

Display reference information about the 5G radio profile **default**.

```
<HUAWEI> display references radio-5g-profile name default
------------------------------------------------------------------------
Reference type  Reference name                  Reference radio
------------------------------------------------------------------------
AP-group        ap-group1                       Radio-0
------------------------------------------------------------------------
Total:1
```

Table 11-33 Description of the **display references radio-5g-profile** command output

Item	Description
Reference type	Type of the profile by which a 5G radio profile is referenced.

Item	Description
Reference name	Name of the profile by which a 5G radio profile is referenced.
Reference radio	Radio to which a 5G radio profile is referenced.

11.1.75 display references regulatory-domain-profile

Function

The **display references regulatory-domain-profile** command displays reference information about a regulatory domain profile.

Format

display references regulatory-domain-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified regulatory domain profile.	The regulatory domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references regulatory-domain-profile** command to view reference information about a regulatory domain profile.

Example

Display reference information about the regulatory domain profile **default**.

```
<HUAWEI> display references regulatory-domain-profile name default
-------------------------------------------------------------
Reference type          Reference name
-------------------------------------------------------------
AP-group                default
AP-group                1
```



```
------------------------------------------------------------------
Total: 2
```

Table 11-34 Description of the **display references regulatory-domain-profile** command output

Item	Description
Reference type	Type of the profile by which a regulatory domain profile is referenced.
Reference name	Name of the profile by which a regulatory domain profile is referenced.

11.1.76 display references softgre-profile

Function

The **display references softgre-profile** command displays reference information about a soft GRE profile.

Format

display references softgre-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified soft GRE profile.	The specified soft GRE profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view reference information about a soft GRE profile.

Example

Display reference information about the soft GRE profile **soft1**.


```
<HUAWEI> display references softgre-profile name soft1
------------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------------
VAP profile                 vap1
------------------------------------------------------------------------------
Total: 1
```

Table 11-35 Description of the **display references softgre-profile** command output

Item	Description
Reference type	Type of the profile by which a soft GRE profile is referenced.
Reference name	Name of the profile by which a soft GRE profile is referenced.

11.1.77 display references ssid-profile

Function

The **display references ssid-profile** command displays reference information about an SSID profile.

Format

display references ssid-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified SSID profile.	The SSID profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references ssid-profile** command to view reference information about an SSID profile.

Example

Display reference information about the SSID profile **default**.

```
<HUAWEI> display references ssid-profile name default
------------------------------------------------------------------------
Reference type                Reference name
------------------------------------------------------------------------
VAP profile                   vap-profile1
------------------------------------------------------------------------
Total:1
```

Table 11-36 Description of the **display references ssid-profile** command output

Item	Description
Reference type	Type of the profile by which an SSID profile is referenced.
Reference name	Name of the profile by which an SSID profile is referenced.

11.1.78 display references vap-profile

Function

The **display references vap-profile** command displays reference information about a VAP profile.

Format

display references vap-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified VAP profile.	The VAP profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references vap-profile** command to view reference information about a VAP profile.

Example

Display reference information about the VAP profile **default**.

```
<HUAWEI> display references vap-profile name default
------------------------------------------------------------------------------
Reference type     Reference name                Reference radio  WLAN ID
------------------------------------------------------------------------------
AP group           group1                        Radio-0          1
------------------------------------------------------------------------------
Total: 1
```

Table 11-37 Description of the **display references vap-profile** command output

Item	Description
Reference type	Type of the profile by which a VAP profile is referenced.
Reference name	Name of the profile by which a VAP profile is referenced.
Reference radio	AP radio by which a VAP profile is referenced.
WLAN ID	WLAN ID of a VAP.

11.1.79 display references vlan pool

Function

The **display references vlan pool** command displays reference information about a VLAN pool.

Format

display references vlan pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Displays reference information about a specified VLAN pool.	The VLAN pool must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view profiles that reference a VLAN pool.

Example

Display reference information about the VLAN pool **pool1**.

```
<HUAWEI> display references vlan pool pool1
--------------------------------------------------------------------------------
Reference type     Reference name                Reference radio  WLAN ID
--------------------------------------------------------------------------------
AP group           default                       Radio-0          1
AP group           default                       Radio-1          1
AP group           default                       Radio-2          1
AP group           default                       Radio-0          2
AP group           default                       Radio-1          2
AP group           default                       Radio-2          2
AP ID              0                             Radio-0          2
AP ID              0                             Radio-1          2
VAP profile        1
user group         123
--------------------------------------------------------------------------------
Total: 10
```

Table 11-38 Description of the **display references vlan pool** command output

Item	Description
Reference type	Type of a profile that references a VLAN pool.
Reference name	Name of a profile that references a VLAN pool.
Reference radio	Radio that references a VLAN pool. This item is displayed only when a VLAN pool is configured as the service VLAN for a VAP profile applied in the AP group radio view or AP radio view.
WLAN ID	WLAN ID that references a VLAN pool. This item is displayed only when a VLAN pool is configured as the service VLAN for a VAP profile applied in the AP group radio view or AP radio view.

11.1.80 display regulatory-domain-profile

Function

The **display regulatory-domain-profile** command displays configuration and reference information about a regulatory domain profile.

Format

display regulatory-domain-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all regulatory domain profiles.	-
name *profile-name*	Displays information about a specified regulatory domain profile.	The regulatory domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display regulatory-domain-profile** command to view configuration and reference information about a regulatory domain profile.

Example

Display information about all regulatory profiles.

```
<HUAWEI> display regulatory-domain-profile all
------------------------------------------------------------
Profile name        Reference
------------------------------------------------------------
default             6
------------------------------------------------------------
Total: 1
```

Table 11-39 Description of the **display regulatory-domain-profile all** command output

Item	Description
Profile name	Regulatory domain profile name.
Reference	Number of times a regulatory domain profile is referenced.

Display information about the regulatory domain profile **default**.

```
<HUAWEI> display regulatory-domain-profile name default
------------------------------------------------------------
```



```
Profile name          : default
Country code          : CN
2.4G dca channel-set  : 1,6,11
5G dca bandwidth      : 20mhz
5G dca channel-set    : 149,153,157,161,165
6G dca bandwidth      : 20mhz
6G dca channel-set    : -
Wideband switch       : enable
Channel load mode     : outdoor
------------------------------------------------------------
```

Table 11-40 Description of the **display regulatory-domain-profile name** command output

Item	Description
Profile name	Regulatory domain profile name.
Country code	Country code. To configure the parameter, run the **country-code** command.
2.4G dca channel-set	2.4G radio calibration channel set. To configure the parameter, run the **dca-channel channel-set** command.
5G dca bandwidth	5G radio calibration bandwidth. To configure the parameter, run the **dca-channel bandwidth** command.
5G dca channel-set	5G radio calibration channel set. To configure the parameter, run the **dca-channel channel-set** command.
6G dca bandwidth	6G radio calibration bandwidth. To configure the parameter, run the **dca-channel bandwidth** command.
6G dca channel-set	6G radio calibration channel set. To configure the parameter, run the **dca-channel channel-set** command.
Wideband switch	Indicates whether the wideband function, that is, the 4.9 GHz frequency band, of the regulatory domain profile is enabled. • enable: The wideband function is enabled. • disable: The wideband function is disabled. To configure this parameter, run the **wideband enable** command.

Item	Description
Channel load mode	Channel load mode. • outdoor: outdoor mode • indoor: indoor mode To configure this parameter, run the **channel-load-mode indoor** command.

11.1.81 display softgre-profile

Function

The **display softgre-profile** command displays configuration and reference information about a soft GRE profile.

Format

display softgre-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all soft GRE profiles.	-
name *profile-name*	Displays information about a specified soft GRE profile.	The specified soft GRE profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check configuration and reference information about soft GRE profiles.

Example

Display information about all soft GRE profiles.


```
<HUAWEI> display softgre-profile all
--------------------------------------------------------------------------------
Profile name                    Reference     IP address
--------------------------------------------------------------------------------
soft1                           0             10.10.1.1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-41 Description of the **display softgre-profile all** command output

Item	Description
Profile name	Name of a soft GRE profile.
Reference	Number of times a soft GRE profile is referenced.
IP address	Tunnel destination address configured in the soft GRE profile.

Display information about the soft GRE profile **soft1**.

```
<HUAWEI> display softgre-profile name soft1
------------------------------------------------------------------
Destination IP-address : 10.10.1.1
Keepalive              : enable
Keepalive period       : 5(s)
Keepalive retry-times  : 3
Untagged VLAN          : 101
------------------------------------------------------------------
```

Table 11-42 Description of the **display softgre-profile name** command output

Item	Description
Destination IP-address	Destination IP address of the soft GRE tunnel. To configure this parameter, run the **destination (soft GRE profile view)** command.
Keepalive	Whether Keepalive detection is enabled for the soft GRE tunnel. To configure this parameter, run the **keepalive** command.
Keepalive period	Interval for sending Keepalive packets. To configure this parameter, run the **keepalive period** *period* command.
Keepalive retry-times	Unreachable counter. To configure this parameter, run the **keepalive period** *period* **retry-times** *retry-times* command.

Item	Description
Untagged VLAN	VLAN tag removed from the soft GRE tunnel packets sent by an AP. To configure this parameter, run the **untagged vlan (soft GRE profile view)** command.

11.1.82 display softgre-tunnel-status

Function

The **display softgre-tunnel-status** command displays soft GRE tunnel information on a specified AP.

Format

display softgre-tunnel-status { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays soft GRE tunnel information on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays soft GRE tunnel information on the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the soft GRE tunnel status and Keepalive information.

Example

Display soft GRE tunnel information on the AP named **area_1**.

```
<HUAWEI> display softgre-tunnel-status ap-name area_1
-------------------------------------------------------------------------------
Destination IP-address          Status     Keepalive    Request    Response
-------------------------------------------------------------------------------
```



```
10.10.1.1                       UP       enable      1         0
------------------------------------------------------------------------------------------------------
```

Table 11-43 Description of the **display softgre-tunnel-status** command output

Item	Description
Destination IP-address	Destination IP address of the soft GRE tunnel. To configure this parameter, run the **destination (soft GRE profile view)** command.
Status	Status of a soft GRE tunnel. • DOWN: When Keepalive detection is enabled, the device detects that the peer end is unreachable and sets the soft GRE tunnel status to **DOWN**. • UP: When Keepalive detection is disabled or Keepalive detection is enabled and the peer is reachable, the device sets the soft GRE tunnel status to **UP**.
Keepalive	Whether Keepalive detection is enabled for the soft GRE tunnel. To configure this parameter, run the **keepalive (soft GRE profile view)** command.
Request	Number of Keepalive request packets sent by the AP.
Response	Number of Keepalive response packets received by the AP.

11.1.83 display ssid-profile

Function

The **display ssid-profile** command displays configuration and reference information about SSID profiles.

Format

display ssid-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all SSID profiles.	-
name *profile-name*	Displays information about a specified SSID profile.	The SSID profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ssid-profile** command to view configuration and reference information about SSID profiles.

Example

Display information about all SSID profiles.

```
<HUAWEI> display ssid-profile all
------------------------------------------------------------------
Profile name  Beacon 2.4G/5G/6G rate(Mbps)  Reference  SSID
------------------------------------------------------------------
default       1/6                         2          GUEST-WLAN
------------------------------------------------------------------
Total: 1
```

Table 11-44 Description of the **display ssid-profile all** command output

Item	Description
Profile name	SSID profile name.
Beacon 2.4G/5G/6G rate(Mbps)	Rate of management frames on each frequency band.
Reference	Number of times an SSID profile is referenced.
SSID	SSID name.

Display information about the SSID profile **default**.

```
<HUAWEI> display ssid-profile name default
------------------------------------------------------------------
Profile ID                      : 0
```



```
SSID                             : GUEST-WLAN
SSID hide                        : disable
Association timeout(min)         : 5
Max STA number                   : 64
Action upon reaching the max STA number : SSID broadcast
Legacy station                   : enable
DTIM interval                    : 1
Beacon 2.4G rate(Mbps)           : 1
Beacon 5G rate(Mbps)             : 6
Beacon 6G rate(Mbps)             : 6
802.11bg basic rate              : 1 6 9
802.11bg support rate            : 1 2 9 12
802.11a basic rate               : 6 9
802.11a support rate             :
Deny-broadcast-probe             : disable
Probe-response-retry num         : 1
802.11r                          : disable
  802.11r authentication         : -
802.11r private                  : disable
802.11r reassociation timeout (s)  : 5
QOS CAR inbound CIR(kbit/s)      : -
QOS CAR inbound PIR(kbit/s)      : -
QOS CAR inbound CBS(byte)        : -
QOS CAR inbound PBS(byte)        : -
U-APSD                           : enable
Active dull client               : disable
Force active dull client         : disable
MU-MIMO                          : disable
MU-MIMO optimize                 : disable
TWT switch                       : disable
QBSS load                        : disable
Single txchain                   : disable
Advertise AP name                : disable
Service guarantee                : performance first
Inter-AC roam switch             : disable
Game-turbo switch                : enable
VHT tx mcs-map nss value         : -
VHT tx mcs-map map value         : -
VHT rx mcs-map nss value         : -
VHT rx mcs-map map value         : -
HE tx mcs-map nss value          : 8
HE tx mcs-map map value          : 11
HE rx mcs-map nss value          : 8
HE rx mcs-map map value          : 11
Beamforming switch               : enable
OFDMA downlink switch            : enable
OFDMA uplink switch              : enable
ER-SU                            : enable
--------------------------------------------------------------------------
WMM EDCA client parameters:
--------------------------------------------------------------------------
      ECWmax  ECWmin  AIFSN  TXOPLimit(32us)
AC_VO  3      2       2        47
AC_VI  4      3       2        94
AC_BE  10     4       3        0
AC_BK  10     4       7        0
--------------------------------------------------------------------------
WMM MUEDCA client parameters:
--------------------------------------------------------------------------
      ECWmax  ECWmin  AIFSN  MUEDCA Timer(8TUs)
AC_VO  3      2       2      1
AC_VI  4      3       2      1
AC_BE  10     4       3      1
AC_BK  10     4       7      1
--------------------------------------------------------------------------
```


Table 11-45 Description of the **display ssid-profile name** command output

Item	Description
Profile ID	ID of an SSID profile.
SSID	SSID name. To configure this parameter, run the **ssid** command.
SSID hide	SSID hiding. To configure this parameter, run the **ssid-hide enable** command.
Association timeout(min)	Association timeout period. To configure this parameter, run the **association-timeout** command.
Max STA number	Maximum number of users. To configure this parameter, run the **max-sta-number (SSID profile view)** command.
Action upon reaching the max STA number	Action to take when the number of access users reaches the maximum. ● SSID hide: hiding the SSID ● SSID broadcast: broadcasting the SSID ● priority-based STA replacement: allowing access of VIP users instead of non-VIP users based on priorities To configure this parameter, run the **reach-max-sta** command.
Legacy station	Whether to permit access of non-HT STAs. To configure this parameter, run the **legacy-station disable** command.
DTIM interval	DTIM interval. To configure this parameter, run the **dtim-interval** command.
Beacon 2.4G rate(Mbps)	Rate at which 2.4 GHz management frames are sent. To configure this parameter, run the **beacon-2g-rate** command.
Beacon 5G rate(Mbps)	Rate at which 5 GHz management frames are sent. To configure this parameter, run the **beacon-5g-rate** command.

Item	Description
Beacon 6G rate(Mbps)	Rate at which 6 GHz management frames are sent. To configure this parameter, run the **beacon-6g-rate** command
802.11bg basic rate	802.11b/g basic rate set. If no information is displayed, no configuration is available and the configuration in the radio profile takes effect. To configure this parameter, run the **dot11bg basic-rate** (SSID profile view) command.
802.11bg support rate	802.11b/g supported rate set. If no information is displayed, no configuration is available and the configuration in the radio profile takes effect. To configure this parameter, run the **dot11bg supported-rate** (SSID profile view) command.
802.11a basic rate	802.11a basic rate set. If no information is displayed, no configuration is available and the configuration in the radio profile takes effect. To configure this parameter, run the **dot11a basic-rate** (SSID profile view) command.
802.11a support rate	802.11a supported rate set. If no information is displayed, no configuration is available and the configuration in the radio profile takes effect. To configure this parameter, run the **dot11a supported-rate** (SSID profile view) command.
Deny-broadcast-probe	Whether an AP is configured not to respond to broadcast Probe Request frames. To configure this parameter, run the **deny-broadcast-probe enable** command.

Item	Description
Probe-response-retry num	Number of times Probe Response packets are retransmitted. To configure this parameter, run the **probe-response-retry** command.
802.11r	802.11r roaming. To configure this parameter, run the **dot11r enable** command.
802.11r authentication	802.11r authentication mode. To configure this parameter, run the **dot11r enable** command.
802.11r proprietary	Whether Huawei's proprietary 802.11r function is enabled. To configure this parameter, run the **dot11r proprietary** command.
802.11r reassociation timeout (s)	802.11r reassociation timeout interval. To configure this parameter, run the **dot11r reassociate-timeout** command.
QOS CAR inbound CIR(kbit/s)	CIR in the QoS CAR profile applied to the inbound direction of an interface, which is the allowed rate at which traffic can pass through. To configure this parameter, run the **qos car (SSID profile view)** command.
QOS CAR inbound PIR(kbit/s)	PIR in the QoS CAR profile applied to the inbound direction of an interface, which is the maximum rate of traffic that can pass through an interface. To configure this parameter, run the **qos car (SSID profile view)** command.
QOS CAR inbound CBS(byte)	CBS in the QoS CAR profile applied to the inbound direction of an interface, which is the average volume of burst traffic that can pass through an interface. To configure this parameter, run the **qos car (SSID profile view)** command.

Item	Description
QOS CAR inbound PBS(byte)	PBS in the QoS CAR profile applied to the inbound direction of an interface, which is the maximum volume of burst traffic that can pass through an interface. To configure this parameter, run the **qos car (SSID profile view)** command.
U-APSD	Whether the U-APSD function is enabled. To configure this parameter, run the **u-apsd enable** command.
Active dull client	Whether the function of preventing terminals from entering energy-saving mode is enabled. To configure this parameter, run the **active-dull-client enable** command.
Force active dull client	Whether the function of forcibly preventing terminals from entering power-saving mode is enabled. To configure this parameter, run the **active-dull-client force enable** command.
MU-MIMO	Whether downlink MU-MIMO scheduling is enabled. To configure this parameter, run the **mu-mimo disable** command.
MU-MIMO optimize	Whether the MU-MIMO optimization function is enabled. To configure this parameter, run the **mu-mimo optimize enable** command.
TWT switch	Whether the TWT function is enabled. To configure this parameter, run the **twt enable** command.
QBSS load	Whether the QBSS load function is enabled. To configure this parameter, run the **qbss-load enable** command.

Item	Description
Single txchain	Whether to enable the single-antenna transmission mode. To configure this parameter, run the **single-txchain enable** command.
Advertise AP name	Whether Beacon frames are enabled to carry the AP name. To configure this parameter, run the **advertise-ap-name enable** command.
Service guarantee	Service guarantee mode. To configure this parameter, run the **service-guarantee** command.
Inter-AC roam switch	Whether inter-AC roaming is enabled. To configure this parameter, run the **inter-ac roam disable** command.
Game-turbo switch	Whether the game turbo function is enabled. To configure this parameter, run the **game-turbo disable** command.
VHT tx mcs-map nss value	Maximum number of spatial streams sent in 802.11ac. To configure this parameter, run the **vht mcs-map (SSID profile view)** command.
VHT tx mcs-map map value	Maximum MCS value of spatial streams sent in 802.11ac. To configure this parameter, run the **vht mcs-map (SSID profile view)** command.
VHT rx mcs-map nss value	Maximum number of spatial streams received in 802.11ac. To configure this parameter, run the **vht mcs-map (SSID profile view)** command.
VHT rx mcs-map map value	Maximum MCS value of spatial streams received in 802.11ac. To configure this parameter, run the **vht mcs-map (SSID profile view)** command.

Item	Description
HE tx mcs-map nss value	Maximum number of spatial streams sent in 802.11ax. To configure this parameter, run the **he mcs-map (SSID profile view)** command.
HE tx mcs-map map value	Maximum MCS value of spatial streams sent in 802.11ax. To configure this parameter, run the **he mcs-map (SSID profile view)** command.
HE rx mcs-map nss value	Maximum number of spatial streams received in 802.11ax. To configure this parameter, run the **he mcs-map (SSID profile view)** command.
HE rx mcs-map map value	Maximum MCS value of spatial streams received in 802.11ax. To configure this parameter, run the **he mcs-map (SSID profile view)** command.
Beamforming switch	Whether the beamforming function is enabled. To configure this parameter, run the **beamforming disable** command. This configuration takes effect only on APs running V200R019C10 or later.
OFDMA downlink switch	Whether downlink OFDMA is enabled. To configure this parameter, run the **ofdma downlink disable** command.
OFDMA uplink switch	Whether uplink OFDMA is enabled. To configure this parameter, run the **ofdma uplink disable** command.
ER-SU	Whether the extended-range single-user (ER SU) function is enabled. To configure this parameter, run the **er-su disable** command.
WMM EDCA client parameters	WMM parameters for STAs. To configure this parameter, run the **wmm edca-client (SSID profile view)** command.
AC_VO	AC_VO packets.

Item	Description
AC_VI	AC_VI packets.
AC_BE	AC_BE packets.
AC_BK	AC_BK packets.
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time.
TXOPLimit(32us)	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger value indicates a longer duration.
WMM MUEDCA client parameters	MU EDCA parameters for STAs. To configure this parameter, run the **wmm mu-edca-client (SSID profile view)** command.
MUEDCA Timer(8TUs)	MU EDCA timer, which indicates the validity duration of MU EDCA parameters. When the timer is 0, the conventional EDCA parameters take effect.

11.1.84 display sta-offline-delay configuration

Function

The **display sta-offline-delay configuration** command displays the STA offline delay configuration.

Format

display sta-offline-delay configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the STA offline delay configuration.

Example

Display the STA offline delay configuration.

```
<HUAWEI> display sta-offline-delay configuration
------------------------------------------------------------------------------
Enable switch                 : disable
Aging time(s)                 : 180
Full station reject switch      : disable
Max number                    : 2048
------------------------------------------------------------------------------
```

Table 11-46 Description of the **display sta-offline-delay configuration** command output

Item	Description
Enable switch	Whether to enable the STA offline delay function. To configure the parameter, run the **sta-offline-delay enable** command.
Aging time(s)	Aging time of the STA offline delay state To configure the parameter, run the **sta-offline-delay aging-time** command.
Full station reject switch	Whether to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum. To configure the parameter, run the **sta-offline-delay full-sta-reject enable** command.
Max number	Maximum number of STAs that are allowed to delay going offline. To configure the parameter, run the **sta-offline-delay max-number** command.

11.1.85 display station

Function

The **display station** command displays access information about STAs.

Format

display station { **ap-group** *ap-group-name* | **ap-name** *ap-name* | **ap-id** *ap-id* | **ssid** *ssid* | **sta-mac** *sta-mac-address* | **vlan** *vlan-id* | **all** }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays STA access information about a specified AP group.	The AP group must exist.
ap-name *ap-name*	Displays STA access information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays STA access information about the AP with a specified ID.	The AP ID must exist.
ssid *ssid*	Displays STA access information about a specified SSID.	The SSID must exist. To specify an SSID starting with a space, include the SSID with double quotation marks (" "). For example, in the SSID **" hello"**, the double quotation marks at the start and end of the SSID occupy two characters. To specify an SSID starting with a double quotation mark ("), enter an escape character (\) before the double quotation mark. For example, in the SSID **\"hello**, the escape character (\) occupies one character.

Parameter	Description	Value
sta-mac *sta-mac-address*	Displays access information about a STA with the specified MAC address.	The STA's MAC address must exist. STA information can be displayed only when the AP associated with the STA is in normal state.
vlan *vlan-id*	Displays STA access information about a specified VLAN.	-
all	Displays access information about all STAs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display station** command to view access information about STAs. You can run the **display access-user** command to view access information about online wired and wireless users. The information includes users' authentication, authorization, and accounting information.

Capabilities of a STA displayed in the **display station sta-mac** *sta-mac-address* command output are negotiated between the STA and AP and are affected by both their capabilities, which may be different from the actual STA capabilities.

Example

Display access information about all STAs.

```
<HUAWEI> display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
--------------------------------------------------------------------------------------------------------
STA MAC         AP ID Ap name       Rf/WLAN  Band  Type  Rx/Tx     RSSI  VLAN  IP address    SSID
Status
--------------------------------------------------------------------------------------------------------
00e0-fc12-3456   0     00e0-fc07-6f80 0/2     2.4G  11n   3/8       -70   10    10.10.10.253  tap1     Normal
--------------------------------------------------------------------------------------------------------
Total: 1 2.4G: 1 5G: 0 6G: 0
```


Table 11-47 Description of the **display station all** command output

Item	Description
STA MAC	MAC address of a STA.
AP ID	AP ID.
Ap name	AP name.
Rf/WLAN	Radio ID/VAP ID.
Band	Frequency band of a radio.
Type	Protocol type of a radio.
Rx/Tx	Rate at which the AP receives packets from the STA/Rate at which the AP sends packets to the STA.
RSSI	RSSI of signals received by an AP from a STA.
VLAN	VLAN ID of a STA.
IP address	IP address of a STA.
SSID	SSID name.
Status	Status of a STA. **Normal** indicates that the STA is in normal state, and **Delay** indicates that the STA is in offline delay state. This item is displayed only when the STA offline delay function is enabled. To enable the STA offline delay function, run the **sta-offline-delay enable** command.

Display access information about a specified STA.

```
<HUAWEI> display station sta-mac 00e0-fcb4-2689
-------------------------------------------------------------------------------
Station MAC-address                      : 00e0-fc12-3456
Station IP-address                       : 10.2.2.254
                                         : FE80::20E:8EFF:FE04:2DEB
Station gateway                          : 10.2.2.2
                                         : FE80::2E97:B1FF:FEB0:6A48
Associated SSID                          : test
Station online time(ddd:hh:mm:ss)        : 000:00:03:14
The upstream SNR(dB)                     : 80.0
The upstream aggregate receive power(dBm)    : -28.0
Station connect rate(Mbps)               : 61
Station connect channel                  : 36
Station inactivity time(ddd:hh:mm:ss)    : 000:00:00:00
Station current state
  Authorized for data transfer           : Yes
  QoS enabled                            : Yes
  HT rates enabled                       : Yes
  Power save mode enabled                : Yes
```



```
  Auth reference held                    : No
  UAPSD enabled                          : No
  UAPSD triggerable                      : No
  UAPSD SP in progress                   : No
  This is an ATH node                    : No
  WDS workaround req                     : No
  WDS link                               : No
  PMF negotiation                        : No
Station's HT capability                  : WQ
Station capabilities                     : E
Station PMF capabilities                 : PMFC=0,PMFR=0
Station VHT capabilities
  256QAM capabilities                    : Yes
  VHT explicit beamforming capabilities  : Yes
  MU-MIMO capabilities                   : Yes
Station HE capabilities
  OFDMA capabilities                     : No
  BSS color capabilities                 : No
  HE SU beamformee capabilities          : No
Station's RM capabilities
  Neighbor Report                        : Yes
  Beacon Passive Measurement             : Yes
  Beacon Active Measurement              : Yes
  Beacon Table Measurement               : Yes
  Link Measurement                       : Yes
  Transmit power adaptation              : Yes
Station EHT capabilities
  MRU capabilities                       : Yes
  BE SU beamformee capabilities          : Yes
  DL MU-MIMO Partial Bandwidth           : Yes
  UL MU-MIMO Partial Bandwidth           : Yes
  MLO capabilities                       : Yes
Station's RSSI(dBm)                      : -28
Station's radio mode                     : 11n
Station's AP ID                          : 0
Station's AP Name                        : area_3
Station's ORU ID                         : -
Station's Radio ID                       : 1
Station's Authentication Method          : Open
Station's Cipher Type                    : NO CIPHER
Station's User Name                      : b8782eb42689
Station's Vlan ID                        : 22
Station's Channel Band-width             : 20MHz
Station's asso BSSID                     : 00e0-fc12-3457
Station's state                          : Asso with auth
Station's QoS Mode                       : WMM
Station's HT Mode                        : HT20
Station's MCS value                      : 9
Station's NSS value                      : 2
Station's Short GI                       : nonsupport
Station's roam state                     : No
HAC CAPWAP IP                            : -
HAP CAPWAP IP                            : 10.23.100.1
Supported band                           : 2.4G/5G
Supported 2.4G channels                  : -
Supported 5G channels                    : 36,40,44,48,52,56,60,64
                                         : 149,153,157,161,165
Supported 6G channels                    : -
802.11k support                          : Yes
802.11r support                          : Yes
802.11r proprietary support              : No
Available for roaming                    : Yes
Sticky station or not                    : No
Aimless roaming support in sticky state  : Yes
Station device type                      : -
Station identify info
  Category name                          : -
  Vendor name                            : -
  Model name                             : -
```



```
  OS                                  : -
U-APSD list:
-------------------------------------------------------
AC-VI          AC-VO         AC-BE         AC-BK
-------------------------------------------------------
not-support  not-support  not-support  not-support
-------------------------------------------------------
-------------------------------------------------------------------------------
```

Table 11-48 Description of the **display station sta-mac** *sta-mac-address* command output

Item	Description
Station MAC-address	MAC address of a STA.
Station IP-address	IP address of a STA.
Station gateway	Gateway address of a STA. **NOTE** If the device obtains the STA's gateway address through DHCP, the parameter displays as the obtained gateway address; otherwise, the parameter displays as 0.0.0.0.
Associated SSID	SSID of a service set with which a STA is associated.
Station online time(ddd:hh:mm:ss)	Online duration of a STA, in the format of ddd:hh:mm:ss.
The upstream SNR(dB)	SNR of a STA received by an AP, in dB.
The upstream aggregate receive power(dBm)	Transmit power of a STA received by an AP, in dBm.
Station connect rate(Mbps)	Connection rate of a STA, in Mbit/s. Affected by wireless environments, antenna angles, and other factors, the actual connection rate of a STA cannot reach the upper limit.
Station connect channel	Channel used by a STA.
Station inactivity time(ddd:hh:mm:ss)	Idle duration of a STA, in the format of ddd:hh:mm:ss.
Station current state	Current status of a STA.
Authorized for data transfer	Whether a STA is authenticated.
QoS enabled	Whether QoS is enabled on a STA.
HT rates enabled	Whether 802.11n is enabled on a STA.
Power save mode enabled	Whether the power saving mode is enabled on a STA.

Item	Description
Auth reference held	Whether the authentication reference flag is set.
UAPSD enabled	Whether UAPSD is enabled.
UAPSD triggerable	UAPSD can be triggered, waiting for a STA to send a trigger frame to the AP.
UAPSD SP in progress	Whether the UAPSD mode is in the service period (SP).
This is an ATH node	Whether the wireless network adapter uses the Atheros chip.
WDS workaround req	Whether the AP uses a patch used to fix bugs of Atheros Owl series chips in WDS scenarios. This item indicates whether the AP uses the patch.
WDS link	STA that is a node on the WDS link.
PMF negotiation	Whether a STA implements the PMF negotiation.
Station's HT capability	HT capability of a STA. ● A: Advanced coding ● W: HT40 channel width ● P: MIMO power save disabled ● Q: Static MIMO power save ● R: Dynamic MIMO power save ● G: Greenfield preamble ● S: Short GI enabled (HT40) ● D: Delayed block ACK ● M: Max A-MSDU size
Station capabilities	Capabilities of a STA. ● E: ESS ● I: IBSS ● c: CF Pollable ● C: CF-Poll Request ● P: Privacy ● S: Short Preamble ● B: PBCC ● A: Channel Agility ● s: Short Slot Time ● D: DSSS-OFDM

Item	Description
Station PMF capabilities	PMF capability of a STA. **PMFC** indicates whether the optional mode is used, and **PMFR** indicates whether the mandatory mode is used. • PMFC=0,PMFR=0: PMF is not supported. • PMFC=1,PMFR=0: PMF in optional mode is used. • PMFC=1,PMFR=1: PMF in mandatory mode is used.
Station VHT capabilities	Whether a STA supports 802.11ac.
256QAM capabilities	Whether a STA supports 256-QAM.
VHT explicit beamforming capabilities	Whether a STA supports 802.11ac explicit beamforming.
MU-MIMO capabilities	Whether a STA supports MU-MIMO.
Station HE capabilities	Whether a STA supports 802.11ax.
OFDMA capabilities	Whether a STA supports OFDMA.
BSS color capabilities	Whether a STA supports BSS Color.
OFDMA RA capabilities	Whether a STA supports OFDMA RA.
TRS capabilities	Whether a STA can receive frames with the TRS field.
BSR capabilities	Whether a STA can receive frames with the BSR field.
DL MU-MIMO partialband capabilities	Whether a STA supports partial-bandwidth downlink MU-MIMO.
UL MU-MIMO fullband capabilities	Whether a STA supports full-bandwidth uplink MU-MIMO.
UL MU-MIMO partialband capabilities	Whether a STA supports partial-bandwidth uplink MU-MIMO.
Dynamic SMPS capabilities	Whether a STA supports Spatial Multiplexing Power Save (SMPS).
HE SU beamformee capabilities	Whether a STA supports HE beamforming.
Station's RM capabilities	Radio management capability of a STA.
Neighbor Report	Whether a STA can obtain information about neighboring APs.

Item	Description
Beacon Passive Measurement	Whether a STA can report information about neighboring APs in passive mode.
Beacon Active Measurement	Whether a STA can report information about neighboring APs in active mode.
Beacon Table Measurement	Whether a STA can report information about neighboring APs in Beacon table mode.
Link Measurement	Whether a STA supports link measurement. ● Yes: supported ● No: not supported
Transmit Power Adaptation	Whether a STA supports TPC. ● Yes: supported ● No: not supported
Station EHT capabilities	802.11be radio management capability of a STA.
MRU capabilities	Whether a STA supports MRU.
BE SU beamformee capabilities	Whether a STA supports SU beamformee.
DL MU-MIMO Partial Bandwidth	Whether a STA supports downlink MU-MIMO.
UL MU-MIMO Partial Bandwidth	Whether a STA supports uplink MU-MIMO.
MLO capabilities	Whether a STA supports MLO.
Station's RSSI(dBm)	RSSI of signals received by an AP from a STA, in dBm.
Station's radio mode	Radio mode of a STA.
Station's AP ID	AP ID associated with a STA.
Station's AP Name	Name of the AP which a STA associates with.
Station's ORU ID	ID of the ORU associated with a STA in a distributed AP scenario. Particularly, if the STA associates with the 2.4 GHz radio, two ORU IDs are displayed, with one of which the STA actually associates.
Station's Radio ID	Radio ID of a STA.

Item	Description
Station's Authentication Method	Authentication mode of a STA.
Station's Cipher Type	Encryption mode of a STA.
Station's User Name	User name of a STA.
Station's Vlan ID	VLAN ID of a STA.
Station's Channel Band-width	Channel bandwidth of a STA.
Station's asso BSSID	BSSID with which a STA is associated.
Station's state	Status of the STA.
Station's QoS Mode	QoS mode of the STA.
Station's HT Mode	HT mode of the STA. ● EHT: 802.11be ● HE: 802.11ax ● VHT: 802.11ac ● HT: 802.11n ● -: 802.11a/b/g
Station's MCS value	The maximum MCS value of the STA.
Station's NSS value	NSS value of the STA. If the STA does not support NSS or the NSS value is 0, a hyphen (-) is displayed.
Station's Short GI	Whether the STA supports the short GI.
Station's roam state	Roaming state of a STA.
HAC CAPWAP IP	CAPWAP IP address for inter-AC communication.
HAP CAPWAP IP	CAPWAP IP address for AP access.
Supported band	Frequency bands supported by the STA.
Supported 2.4G channels Supported 5G channels Supported 6G channels	Channel set supported by a STA. **NOTE** If **-** is displayed, possible causes include: ● The AP version is too early to report channels supported by STAs. ● The STA cannot report the support channels IE field.
802.11k support	Whether a STA supports 802.11k.
802.11r support	Whether a STA supports 802.11r.

Item	Description
802.11r proprietary support	Whether the STA supports Huawei proprietary 802.11r over-the-DS roaming.
802.11v support	Whether a STA supports 802.11v.
Available for roaming	Whether a STA can trigger the roaming process.
Sticky station or not	Whether a STA is a sticky terminal.
Station device type	Identified STA type.
Aimless roaming support in sticky state	Whether a STA is forced to roam to the target AP.
Station identify info	STA information identified by the device.
Category name	STA category identified by the device.
Vendor name	STA vendor identified by the device.
Model name	STA model identified by the device.
OS	STA operating system identified by the device.
U-APSD list	U-APSD list.
AC-VI	Whether U-APSD takes effect on AC_VI packets.
AC-VO	Whether U-APSD takes effect on AC_VO packets.
AC-BE	Whether U-APSD takes effect on AC_BE packets.
AC-BK	Whether U-APSD takes effect on AC_BK packets.

11.1.86 display station assoc-info ap-offline-record

Function

The **display station assoc-info ap-offline-record** command displays information about STAs that connect to the APs in fault state.

Format

display station assoc-info ap-offline-record { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Displays information about STAs that connect to all APs in fault state.	-
ap-name *ap-name*	Displays information about STAs that go online on the AP with a specified name in fault state.	The AP name must exist.
ap-id *ap-id*	Displays information about STAs that go online on the AP with a specified ID in fault state.	The AP ID must exist.
radio *radio-id*	Displays information about STAs that connect to a specified radio of an AP in fault state.	The radio ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When link faults occur between the APs and AC, the APs in fault state allow access of new STAs and log the STA information. When the link between the APs and AC is re-established, the APs disconnect these STAs and send the STA information to the AC. You can run the **display station assoc-info ap-offline-record** command on the AC to check information about the STAs that connect to the APs in fault state.

Prerequisite

The APs in fault state have been enabled to allow access of new STAs using the **keep-service enable allow new-access** command.

Example

Display information about STAs that connect to all APs in fault state.

```
<HUAWEI> display station assoc-info ap-offline-record all
Offline Station information list:
--------------------------------------------------------------------------------
STA MAC         AP name   RADIO ID  SSID
--------------------------------------------------------------------------------
00e0-fc12-3456  ap1       0         SSID_MYWLAN
--------------------------------------------------------------------------------
Total: 1
```


Table 11-49 Description of the **display station assoc-info ap-offline-record** command output

Item	Description
STA MAC	MAC address of a STA.
AP name	Name of the AP that the STA connects to.
RADIO ID	ID of the radio that the STA connects to.
SSID	SSID that the STA connects to.

11.1.87 display station online-fail-record

Function

The **display station online-fail-record** command displays records of STAs' failures to go online.

Format

display station online-fail-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac-address* }

Parameters

Parameter	Description	Value
all	Displays going-online failure records of all STAs.	-
ap-name *ap-name*	Displays records of STAs' failures to go online on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays records of STAs' failures to go online on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac-address*	Displays online failure records of the STA with the specified MAC address.	The STA's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a STA fails to go online, you can run the command to check the failure reason, which helps locate the fault.

After the number of records of STAs' failures to go online reaches the maximum that can be stored, new records overwrite existing ones.

Example

Display online failure records of all STAs.

```
<HUAWEI> display station online-fail-record all
Reason distribution
-------------------------------------------------------------------------------
Reason                                                  Count Percent
-------------------------------------------------------------------------------
The key is incorrect or the STA uses the cached PMK.        1     100.00%
-------------------------------------------------------------------------------
Total Count: 1

Recent records
Rf/WLAN: Radio ID/WLAN ID
--------------------------------------------------------------------------------
STA MAC        AP ID Ap name  Rf/WLAN    Last record time          Reason
--------------------------------------------------------------------------------
00e0-fc12-3456 0     area_11  0/1        2018-04-11/15:53:18       The key is incorrect or the STA uses the
cached PMK.
--------------------------------------------------------------------------------
Total stations: 1 Total records: 1
```

Table 11-50 Description of the **display station online-fail-record** command output

Item	Description
Reason distribution	Distribution of STA going-online failure reasons. All the reasons after the reasons listed in **Table 11-51** are counted as **Other Reasons**. • The authentication request times out.
Count	Number of times that a reason is displayed.
Percent	Percentage of a reason.
Recent records	Recent records of reasons for the STA's failures to go online.
Radio ID/WLAN ID	ID of the radio/VAP to which the STA fails to connect.
STA MAC	MAC address of the STA that fails to go online.

Item	Description
AP ID	ID of the AP on which the STA fails to go online.
Ap name	Name of the AP on which the STA fails to go online.
Last record time	Last time when the STA failed to go online.
Reason	Reason for the STA's failure to go online. For details about STA online failure reasons and handling suggestions, see **Table 11-51**. For reasons of access authentication failures, see **Common Causes for Access Authentication Failures** in *Huawei S Series Campus Switches Troubleshooting Guide*. For troubleshooting methods, see **STAs Fail to Associate with a WLAN** in the *Troubleshooting Guide*.

Table 11-51 STAs' going-online failure reasons and handling suggestions

Reason Why a STA Fails to Go Online	Suggestion
The number of STAs exceeds the physical specifications allowed by the AP.	Expand the network capacity or retain the current configuration as required.
The number of associated STAs exceeds the maximum allowed by the AC.	Expand the WLAN capacity.
The STA associates with a heavily loaded radio.	Check whether the load balancing configuration is proper.
The STA is in the dynamic blacklist.	Check the attack records and check whether the STA has initiated attacks.
The STA's SNR is below the user CAC threshold.	Check whether the SNR-based user CAC threshold is properly set. To modify this threshold, run the **uac client-snr threshold** command and reassociate the STA with the WLAN. Alternatively, determine the STA location and provide coverage to the location.

Reason Why a STA Fails to Go Online	Suggestion
The number of STAs exceeds the maximum allowed by the AP.	Configure load balancing or expand the network capacity.
The number of STAs exceeds the maximum allowed in the VAP reported by the AP.	Increase the maximum number of users on the VAP or expand the WLAN capacity.
The STA does not send an authentication request before associating with the network.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The key is incorrect or the STA uses the cached PMK.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to receive the handshake packet (2/4) from the STA.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to receive the handshake packet (4/4) from the STA.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (start negotiation failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (MAC address authentication failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (WPA key negotiation failure).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
The authentication request times out.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
STA authentication times out.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid association request packet.	Reassociate the STA with the network. If this fault persists, the STA may be incompatible. Contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
The encryption mode is inconsistent on the STA and AP.	Check whether the encryption mode is consistent on the STA and AP.
Authentication fails in the association stage.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA is not authenticated.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The AP does not support the rate set specified in the association request packet of the STA.	Modify the basic rate set and supported rate set in the radio profile and reassociate the STA with the network.
The encryption algorithm is inconsistent on the STA and AP.	Check whether the encryption algorithm is consistent on the STA and AP.
Failed to decrypt the challenge packet.	Reassociate the STA with the network or check whether the STA works properly. If this fault persists, contact technical support personnel.
Access from legacy STAs is denied.	Check whether the configuration for denying access of legacy STAs is required. To modify this configuration, run the **undo legacy-station disable** command to permit access of legacy STAs.
The WMM capability of the STA and VAP does not match.	Check whether WMM is forcibly enabled in the radio profile or check the specified configuration of the STA.
STAs have a compatibility issue(Incorrect network type flag carried by STAs) .	Check whether the STA works properly. If so, reassociate the terminal with the network. If this fault persists, contact technical support personnel.
STAs have a compatibility issue(STAs do not support short timeslots).	Check whether the STA supports the 802.11g protocol.
STAs have a compatibility issue(STAs do not support DFS.)	Check whether the STA supports the 802.11h protocol.
The STA is not in the global whitelist.	Check whether the STA needs to be added to the global whitelist.
The STA is in the global blacklist.	Check whether the STA needs to be added to the global blacklist.

Reason Why a STA Fails to Go Online	Suggestion
The STA is not in the VAP's whitelist.	Check whether the STA needs to be added to the VAP's whitelist.
The STA is in the VAP's blacklist.	Check whether the STA needs to be added to the VAP's blacklist.
The association or reassociation packet check fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The number of users exceeds the maximum allowed on the VAP defined by the AC.	Expand the network capacity or run the **max-sta-number** command to increase the maximum number of STAs associated with the VAP.
The Navi AC status is abnormal.	Check the configuration and the network to Navi AC.
VAP configurations on the Local AC and Navi AC are different.	Check the VAP configurations on the Local AC and Navi AC. Check items are as follows: • STA authentication access mode. • SSID.
The number of associated STAs exceeds the maximum specifications of the Navi AC.	Expand the WLAN capacity.
Failed to check the configuration during STA association.	Contact technical support personnel.
Batch backup is in progress. STA access is denied.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
STA access failed due to other reasons.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Reassociation denied.	No action is required.
During roaming association, the SSID is inconsistent with that before roaming.	Check whether the SSID is the same before and after roaming. If this fault persists, contact technical support personnel.
During roaming association, the authentication mode is inconsistent with that before roaming.	Check whether the authentication mode is the same before and after roaming. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
During roaming association, the STA status is abnormal.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA fails the roaming check due to other reasons.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA uses a static IP address.	Check whether the static IP address is configured by the user. If so, configure the STA to dynamically obtain an IP address.
The number of STAs exceeds the UAC threshold of the radio.	Check whether the CAC threshold based on the number of users is properly set. To modify this threshold, run the **uac client-number threshold** command and reassociate the STA with the WLAN.
The channel utilization of the radio has reached the upper threshold.	Check whether the user CAC threshold based on the channel utilization is properly set. To modify this threshold, run the **uac channel-utilization threshold** command and reassociate the STA with the WLAN.
Exceeded the maximum number of users on the central AP.	Expand the WLAN capacity.
Authentication fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The encryption mode used by STAs is different from that used by the VAP.	Check the encryption modes used by STAs and the VAP.
The possible cause is that the STA configuration is incorrect, the signal quality on the air interface is low, or the AC forces the STA to reassociate with the network to ensure uninterrupted STA services.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The client capability does not match.	The client capability does not meet the requirements. Upgrade the client version or Wi-Fi version.
Compatibility problems exist on the wireless client. (The HT capability carried by the client is incorrect).	Upgrade the STA version or Wi-Fi module version, or run the **undo legacy-station disable** command to permit access of non-HT STAs.

Reason Why a STA Fails to Go Online	Suggestion
The client access is restricted temporarily.	To allow a wireless client to access a better AP, temporarily restrict the client to access this AP. It is normal if the terminal can connect to a better AP. If a client fails to connect to an AP for multiple consecutive times, check whether APs need to be added.
Received an Authentication frame with authentication transaction sequence number out of expected sequence.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid RSNE capabilities.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Cipher suite rejected because of security policy.	Check whether the encryption mode and key configurations on the wireless terminal are correct. If this fault persists, contact technical support personnel.
Invalid pairwise master key identifier(PMKID).	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid group cipher.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid pairwise cipher.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid MDE.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid FTE.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Others reason.	Contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
802.11r EAPOL Msg 2/4 did not contain R1 name.	Check whether the station has some compatibility problems and please disable dot1x reauthenticate when enable 802.11r. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data(2/4) is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data(4/4) is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(fail to send the handshake packet).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
The MAC address of the access user is different from that configured for the PPSK account.	Run the **display wlan ppsk-user all** command to check whether any PPSK account allows the access from this MAC address. If so, use this PPSK account for access. If not, configure a PPSK account mapping this MAC address and use the new PPSK account for access.
The PPSK account does not exist.	Run the **display wlan ppsk-user all** command to check whether any PPSK account maps the access SSID. If not, create the PPSK account and bind it to the SSID.
The number of PPSK users exceeds the maximum value.	Run the **display wlan ppsk-user all** command to query the maximum number of access users supported by the PPSK account, and then modify the maximum number of access users as required.
The PPSK account expires.	Run the **display wlan ppsk-user all** command to check the timeout period of the PPSK account, and change it to a valid time.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (message 2/4 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 1/2 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (start unicast negotiation fails because of incorrect input parameters).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (start multicast negotiation fails because of incorrect input parameters).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/4 authentication mode or encryption type mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 authentication mode or encryption type mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/2).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of WPA data packets).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (invalid length of the message 4/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 2/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 4/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 2/2).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 4/4 packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/2 packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 2/4 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 4/4 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 2/2 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/4 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (message 4/4 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/2 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 2/4 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 4/4 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 2/2 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 MIC verification failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/2 MIC verification failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (packet length calculation failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the EAP packet length is 0).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the EAP packet is too long).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (the key body length of EAP packets is 0).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the EAP packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (incorrect EAP packet descriptor).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid EAP packet type).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (PMK parse failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between the PMK and PMKR1Name).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the type is not FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid FTIE length).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between Anonce and FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between Snonce and FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (MIC generation failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (failure to modify the rsnie field).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (failure to fill FTIE data).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
WAPI authentication times out.	Check the network quality or reassociate the STA with the network. If this fault persists, contact technical support personnel.
WAPI authentication fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (re-authentication failure).	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (failure to fill the start negotiation message).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (authentication failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (failure to fill the start negotiation message).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (start negotiation failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (failure to receive EAP key packets).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (MAC address authentication processing error).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (access security processing failure).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication is rejected because an Anti-CloggingToken is required.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication is rejected because the offered finite cyclic group is not supported.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Robust management frame policy violation	Check whether the encryption mode and pmf configuration are correct on the client.
High-reliability air interface slicing is enabled but is not supported by STA.	Associate the STA with an SSID on which high-reliability air interface slicing is not enabled.

11.1.88 display station offline-record

Function

The **display station offline-record** command displays STAs' going-offline records.

Format

display station offline-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac* }

Parameters

Parameter	Description	Value
all	Displays all STAs' going-offline records.	-
ap-name *ap-name*	Displays STAs' going-offline records on the AP with a specified name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Displays STAs' going-offline records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac*	Displays the going-offline records of a specified STA.	The STA's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a STA goes offline, you can use this command to check the reason why the STA goes offline.

A maximum of three going-offline records can be stored for each STA.

Example

Display all STAs' going-offline records.

```
<HUAWEI> display station offline-record all
Reason distribution
-------------------------------------------------------------------------------
Reason                                                  Count Percent
-------------------------------------------------------------------------------
The STA ages out.                                           1  14.29%
Other Reasons.                                              6  85.71%
-------------------------------------------------------------------------------
Total Count: 7

Recent records
Rf/WLAN: Radio ID/WLAN ID
-------------------------------------------------------------------------------
STA MAC         AP ID Ap name        Rf/WLAN   Last record time        Reason
-------------------------------------------------------------------------------
00e0-fc3f-3db9  0     00e0-fc99-9880 1/3       2018-04-18/12:10:26     The STA is deauthenticated.
00e0-fc8e-8fa0  0     00e0-fc99-9880 0/2       2018-04-18/07:17:40     The STA disassociates with the
network.
00e0-fcd2-efc4  0     00e0-fc99-9880 1/3       2018-04-19/02:34:03     The STA disassociates with the
network.
                0     00e0-fc99-9880 1/4       2018-04-18/08:36:35     The STA disassociates with the
network.
                0     00e0-fc99-9880 1/4       2018-04-18/08:35:30     AAA cut command
00e0-fcc9-8a72  0     00e0-fc99-9880 0/2       2018-04-18/06:47:30     The STA disassociates with the
network.
00e0-fcb4-1750  0     00e0-fc99-9880 0/2       2018-04-18/14:06:41     The STA ages out.
-------------------------------------------------------------------------------
Total stations: 5 Total records: 7
```


Table 11-52 Description of the **display station offline-record** command output

Item	Description
Reason distribution	Distribution of reasons of STAs going offline. All the reasons after the reasons listed in **Table 11-53** are counted as **Other Reasons**. • The STA ages out.
Count	Number of times that a reason is displayed.
Percent	Percentage of a reason.
Recent records	Recent reason records of STAs' going-offline.
STA MAC	MAC address of a STA.
AP ID	ID of the AP from which STAs go offline.
Ap name	Name of the AP from which STAs go offline.
Radio ID/WLAN ID	ID of the radio or WLAN ID of the VAP from which a STA goes offline.
Last record time	Time when the STA went offline last time.
Reason	Reason why the STA went offline. For description of offline reasons and handling suggestions, see **Table 11-53**.For reasons of access authentication failures, see **Common Causes for Access Authentication Failures** in *Huawei S Series Campus Switches Troubleshooting Guide*. For troubleshooting methods, see **A STA Goes Offline Unexpectedly** in the *Troubleshooting Guide*.
Total stations	Total number of STAs.
Total records	Total number of STA offline records.

Table 11-53 Possible reasons and suggestions for STAs to go offline

Reason Why a STA Goes Offline	Suggestion
STA entry addition times out or fails.	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails in the association stage.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The configuration is modified.	Check whether configuration modification records exist.
Roaming check failed(on the eSAP).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Roaming failed(because of a roaming entry failure on the forwarding side or a failure to obtain the configuration).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The AP is faulty.	Check the reason why the AP goes offline, and rectify the fault accordingly. For reasons why an AP goes offline, see **display ap offline-record**.
The AP is deleted.	No action is required.
Failed to synchronize user entries between the AP and AC.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to synchronize user entries in a mobility group.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
A tunnel between ACs goes Down.	Check the network between the ACs.
The home AP goes offline or a network fault occurs.	Reassociate the STA with another AP. If this fault persists, contact technical support personnel.
The home AP is deleted.	Reassociate the STA with another AP. If this fault persists, contact technical support personnel.
The home VAP is deleted.	Reassociate the STA with another VAP. If this fault persists, contact technical support personnel.
The AC forcibly disconnects idle STAs.	Check whether this function is required. If so, no action is required. If not, run the **undo idle-cut** command in the service scheme view to modify the configuration.

Reason Why a STA Goes Offline	Suggestion
Roaming check failed because the user left the current AC during inter-AC roaming.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The keepalive packet on the home AP times out.	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
The keepalive packet between ACs times out.	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Layer 3 roaming is disabled.	Reassociate the STA with the network or enable Layer 3 roaming.
The STA MAC is added to the STA blacklist.	Verify that the STA needs to be added to the blacklist.
The STA disassociates with the network.	Check whether the STA actively goes offline or whether the STA is faulty.
The STA is deauthenticated.	Check whether the STA actively goes offline or whether the STA is faulty.
The VAP goes down because the configuration is modified.	Check whether configuration change records exist in the log.
The STA is added to the dynamic blacklist.	Check whether the STA is an attacker.
The signal strength is too low.	Check whether the threshold for quickly disconnecting STAs by smart roaming is correctly configured, and check whether the WLAN coverage area is sufficient.
No control entry exists.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
No Wi-Fi entry exists.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA roams between ACs.	No action is required.

Reason Why a STA Goes Offline	Suggestion
The STA associates or reassociates with the network but does not send a DHCP Discover message. The STA reassociates with the network but does not send a DHCP request message.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA ages out.	No action is required.
A STA goes offline properly.	No action is required.
Failed to synchronize user entries between WMP and eSAP.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA roams out of the device.	No action is required.
A STA goes offline unexpectedly.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
During inter-AC roaming, the SSID is inconsistent with that before roaming.	Check whether the SSID is the same before and after roaming. If this fault persists, contact technical support personnel.
The STA fails the roaming security check.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA fails the roaming status check.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA fails the roaming check due to other reasons.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to add FPI item.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The device in NAT mode does not support roaming.	Reassociate the STA with the network or reconfigure the network mode.
Layer 3 roaming is disabled(delay offline).	Reassociate the STA with the network or enable Layer 3 roaming.
Fail to send IPC to UCM reporting auth request.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Fail to send IPC to UCM reporting roam request.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Station roam between normal and backup AP.	No action is required.

Reason Why a STA Goes Offline	Suggestion
The PPSK configuration is modified.	Check whether the modification record can be found in the log.
Exceeded the maximum number of login STAs supported by the PPSK account.	Check the maximum number of login STAs supported by the PPSK account.
Failed to synchronize user entries between Local AC and Navi AC.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The remotely authenticated STA is disconnected after an active/standby switchover in the Local AC dual-link networking.	No action is required.
VAP configurations on the Navi AC is modified.	No action is required.
Inter-ac roaming is disabled.	No action is required.
Users go offline due to WDS link disconnection or other unknown reasons (reported by Wi-Fi).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The number of users exceeds the specifications (insufficient key slots).	Expand the AP capacity or reassociate the STA with another AP.
A user exception is detected.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA does not respond.	Check whether the STA works properly.
The STA rate is too low.	Check whether the threshold for quickly disconnecting STAs by smart roaming is correctly configured, and check whether the WLAN coverage area is sufficient.
The STA uses a bogus IP address.	Configure the STA to automatically obtain an IP address.
The AP goes online again.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Multicast key handshake failure.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Reporting the PMK negotiation result to the AC times out.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA disassociates with the network (delay offline).	Check whether the STA actively goes offline or whether the STA is faulty.
The STA is deauthenticated (delay offline).	Check whether the STA actively goes offline or whether the STA is faulty.
The STA ages out (delay offline).	No action is required.
The STA IP address changes after roaming.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
AP restores connection from escape mode.	No action is required.
The soft-GRE tunnel goes down.	Check the connectivity to the peer end of the soft-GRE tunnel. If this fault persists, contact technical support personnel.
Higher-priority STAs access the network.	Configure the STA as a high-priority STA, or increase the user CAC threshold or the maximum number of STAs on a VAP.
The number of STAs reached the CAC or VAP threshold.	Increase the user CAC threshold or the maximum number of STAs on a VAP.
The possible cause is that the STA configuration is incorrect, the signal quality on the air interface is low, or the AC forces the STA to reassociate with the network to ensure uninterrupted STA services.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The key is incorrect or the STA uses the cached PMK.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to receive the handshake packet (2/4) from the STA.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to receive the handshake packet (4/4) from the STA.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
802.11r EAPOL Msg 2/4 did not contain R1 name.	Check whether the station has some compatibility problems and please disable dot1x reauthenticate when enable 802.11r. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data(2/4) is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data(4/4) is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(fail to send the handshake packet).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
The MAC address of the access user is different from that configured for the PPSK account.	Run the **display wlan ppsk-user all** command to check whether any PPSK account allows the access from this MAC address. If so, use this PPSK account for access. If not, configure a PPSK account mapping this MAC address and use the new PPSK account for access.
The PPSK account does not exist.	Run the **display wlan ppsk-user all** command to check whether any PPSK account maps the access SSID. If not, create the PPSK account and bind it to the SSID.
The number of PPSK users exceeds the maximum value.	Run the **display wlan ppsk-user all** command to query the maximum number of access users supported by the PPSK account, and then modify the maximum number of access users as required.
The PPSK account expires.	Run the **display wlan ppsk-user all** command to check the timeout period of the PPSK account, and change it to a valid time.
Key negotiation fails (message 2/4 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 1/2 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Key negotiation fails (start unicast negotiation fails because of incorrect input parameters).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (start multicast negotiation fails because of incorrect input parameters).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/4 authentication mode or encryption type mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 authentication mode or encryption type mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/2).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of WPA data packets).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 4/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 2/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 4/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 2/2).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Key negotiation fails (invalid length of the message 4/4 packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/2 packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 2/4 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 4/4 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 2/2 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/4 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/2 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 2/4 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 4/4 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 2/2 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 MIC verification failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/2 MIC verification failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Key negotiation fails (packet length calculation failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the EAP packet length is 0).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the EAP packet is too long).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the key body length of EAP packets is 0).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the EAP packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (incorrect EAP packet descriptor).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid EAP packet type).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (PMK parse failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between the PMK and PMKR1Name).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the type is not FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid FTIE length).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between Anonce and FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between Snonce and FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Key negotiation fails (MIC generation failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (failure to modify the rsnie field).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (failure to fill FTIE data).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
WAPI authentication times out.	Check the network quality or reassociate the STA with the network. If this fault persists, contact technical support personnel.
WAPI authentication fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (re-authentication failure).	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (failure to fill the start negotiation message).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (start negotiation failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (authentication failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (failure to fill the start negotiation message).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (start negotiation failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (failure to receive EAP key packets).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (MAC address authentication processing error).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (MAC address authentication failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
The authentication request times out.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (WPA key negotiation failure).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails (access security processing failure).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The AAA deletes the STA.	Check whether the AAA configuration and STA authentication information are both correct. If this fault persists, contact technical support personnel.
High-reliability air interface slicing is enabled or disable.	Associate the STA with an SSID on which high-reliability air interface slicing is not enabled.
Service tunnel VLAN is changed.	No action is required.

11.1.89 display station online-track

Function

The **display station online-track** command displays online time information about a STA.

Format

display station online-track *sta-mac-address*

Parameters

Parameter	Description	Value
sta-mac-address	Displays online time information about the STA with a specified MAC address.	The specified MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view online time information about a STA.

Example

Display online time information about a specified STA.

```
<HUAWEI> display station online-track 00e0-fc08-9abf
--------------------------------------------------------------------------------
Event         Event Start(hh:mm:ss)       Event End(hh:mm:ss)      Cost(ms)
--------------------------------------------------------------------------------
Association   14:20:28                     14:20:28                 10
Auth          14:20:28                    14:20:30                 2240
WPA           14:20:30                    14:20:31                 330
DHCP          14:20:31                    14:20:31                 10
--------------------------------------------------------------------------------
Total cost: 2590ms
```

Table 11-54 Description of the **display station online-track** *sta-mac-address* command output

Item	Description
Event	Event type. The values are as follows: • Association: STA association • Auth: STA authentication • WPA: WPA key negotiation • DHCP: STAs obtaining IP addresses through DHCP
Event Start(hh:mm:ss)	Time when the event starts.
Event End(hh:mm:ss)	Time when the event ends.
Cost(ms)	Duration of the event.
Total cost	Total duration of all events.

11.1.90 display station statistics

Function

The **display station statistics** command displays statistics information about STAs.

Format

display station statistics [**sta-mac** *sta-mac-address* | **ap-name** *ap-name* | **ap-id** *ap-id*]

Parameters

Parameter	Description	Value
sta-mac *sta-mac-address*	Displays statistics information about a STA with a specified MAC address.	The STA's MAC address must exist.
ap-name *ap-name*	Displays statistics information about STAs on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays statistics information about STAs on the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display station statistics** command to view statistics information about STAs.

- If no parameter is specified, statistics information about all STAs associated with the AC is displayed.
- If an AP is specified by **ap-name** or **ap-id**, the number of STAs associated with, disassociated from, and reassociated with the AP is displayed.
- If a STA is specified by **sta-mac**, the number of packets and packet transmission rate between the STA and an AP are displayed.

Prerequisites

- To view statistics information about a STA specified by **sta-mac**, ensure that the STA has been associated with an AP.
- To view statistics information about STAs associated with an AP specified by **ap-name** or **ap-id**, ensure that the AP has been added to the AC and is in normal state.

Example

Display statistics information about all STAs.

```
<HUAWEI> display station statistics
------------------------------------------------------------------------------
 Successful associations on the AC                          :0
 AC authentication failures due to a password error         :0
 AC authentication failures due to an invalid algorithm     :0
 AC authentication failures due to timeout                  :0
 AC authentication failures due to rejection                :0
 AC authentication failures due to other reasons            :0
 Sticky STAs detected                                       :0
```



```
Online sticky STAs                                  :0
Sticky STA rate(%)                                  :-
Total number of roamings triggered by sticky STAs          :0
Number of roamings triggered by sticky STAs               :0
Sticky STA-triggered roaming success rate(%)              :-
Unavailable to trigger roam number                       :0
Unavailable to trigger roam rate(%)                      :-
STAs supporting neighbor report                         :0
STAs supporting beacon report                           :0
   Beacon passive measurement                            :0
   Beacon active measurement                            :0
   Beacon table measurement                             :0
2.4G-only STAs                                     :0
5G-only STAs                                       :0
6G-only STAs                                       :0
2.4G and 5G STAs                                     :0
2.4G, 5G and 6G STAs                                  :0
Online STAs                                        :0
   STAs associated with 2.4G band                       :0
   STAs associated with 5G band                        :0
   STAs associated with 6G band                        :0
--------------------------------------------------------------------------------
```

Table 11-55 Description of the **display station statistics** command output

Item	Description
Successful associations on the AC	Total number of successful link authentications on the AC. Every time a STA initiates a link authentication request and passes the authentication, the counter is incremented by 1. If the same STA initiates multiple authentication requests and passes all authentications, the counter is incremented cumulatively.
AC authentication failures due to a password error	Number of authentication failures due to the incorrect password.
AC authentication failures due to an invalid algorithm	Number of authentication failures due to the invalid authentication algorithm.
AC authentication failures due to timeout	Number of authentication failures due to timeout.
AC authentication failures due to rejection	Number of authentication failures due to rejected access to the AC.
AC authentication failures due to other reasons	Number of authentication failures due to other reasons.
Sticky STAs detected	Number of sticky STAs.
Online sticky STAs	Number of online sticky STAs.
Sticky STA rate(%)	Ratio of the number of sticky STAs to the total number of STAs.

Item	Description
Total number of roamings triggered by sticky STAs	Total number of the triggered smart roaming times.
Number of roamings triggered by sticky STAs	Number of the successfully triggered smart roaming times.
Sticky STA-triggered roaming success rate(%)	Success rate of triggered smart roaming.
Unavailable to trigger roam number	Number of STAs that cannot roam on the AC.
Unavailable to trigger roam rate(%)	Ratio of the number of sticky STAs that cannot roam to the total number of STAs on the AC.
STAs supporting neighbor report	Number of STAs that can obtain information about neighboring APs.
STAs supporting beacon report	Number of STAs that can report information about neighboring APs through the Beacon Report mechanism.
Beacon passive measurement	Number of STAs that can report information about neighboring APs in passive mode.
Beacon active measurement	Number of STAs that can report information about neighboring APs in active mode.
Beacon table measurement	Number of STAs that can report information about neighboring APs in Beacon table mode.
2.4G-only STAs	Number of STAs that support only the 2.4 GHz frequency band.
5G-only STAs	Number of STAs that support only the 5 GHz frequency band.
6G-only STAs	Number of STAs that support only the 6 GHz frequency band.
2.4G and 5G STAs	Number of STAs that support only the 2.4 GHz and 5 GHz frequency bands.
2.4G, 5G and 6G STAs	Number of STAs that support the 2.4 GHz, 5 GHz, and 6 GHz frequency bands.
Online STAs	Number of online STAs.

Item	Description
STAs associated with 2.4G band	Number of STAs associated with the 2.4 GHz radio. The number of STAs of different types is displayed, including 802.11b, 802.11g, 802.11be 20 MHz, 802.11be 40 MHz, 802.11ax 20 MHz, 802.11ax 40 MHz, 802.11n 20 MHz, and 802.11n 40 MHz STAs.
STAs associated with 5G band	Number of STAs associated with the 5 GHz radio. The number of STAs of different types is displayed, including 802.11a, 802.11n 20 MHz, 802.11n 40 MHz, 802.11be 20 MHz, 802.11be 40 MHz, 802.11be 80 MHz, 802.11be 160 MHz, 802.11be 320 MHz, 802.11ax 20 MHz, 802.11ax 40 MHz, 802.11ax 80 MHz, 802.11ax 160 MHz, 802.11ac 20 MHz, 802.11ac 40 MHz, 802.11ac 80 MHz, and 802.11ac 160 MHz STAs.
STAs associated with 6G band	Number of STAs associated with the 6 GHz radio. The number of STAs of different types is displayed, including 802.11be 20 MHz, 802.11be 40 MHz, 802.11be 80 MHz, 802.11be 160 MHz, 802.11be 320 MHz, 802.11ax 20 MHz, 802.11ax 40 MHz, 802.11ax 80 MHz, and 802.11ax 160 MHz STAs.

Display statistics information about the STA with the MAC address 00e0-fc33-4455.

```
<HUAWEI> display station statistics sta-mac 00e0-fc33-4455
-------------------------------------------------------------------
  Packets sent to the station                        : 7
  Packets received from the station                  : 40
  Bytes sent to the station                          : 1170
  Bytes received from the station                    : 3911
  Wireless data rate sent to the station(kbps)       : 0
  Wireless data rate received from the station(kbps) : 0
  Trigger roam total                                 : 0
  Trigger roam failed                                : 0
  STA power save percent                             : 0%
-------------------------------------------------------------------------------
```

Table 11-56 Description of the **display station statistics sta-mac** *sta-mac-address* command output

Item	Description
Packets sent to the station	Number of packets sent to the STA.

Item	Description
Packets received from the station	Number of packets received from the STA.
Bytes sent to the station	Number of bytes sent to the STA.
Bytes received from the station	Number of bytes received from the STA.
Wireless data rate sent to the station(kbps)	Rate at which packets are sent to the STA, in kbit/s.
Wireless data rate received from the station(kbps)	Rate at which packets are received from the STA, in kbit/s.
Trigger roam total	Total number of smart roaming times.
Trigger roam failed	Number of smart roaming failures.
STA power save percent	Percentage of power saved on the STA.

Display STA statistics information of a specified AP.

```
<HUAWEI> display station statistics ap-name N1-1
--------------------------------------------------------------------------------
  Total online time of STAs (seconds)                 :0
  STAs associated with the AP                         :0
  Association requests                                :0
  Successful association requests                     :0
  Rejected association requests                       :0
  Failed association requests                         :0
  Repeated association requests                       :0
  Reassociation requests                              :0
  Successful reassociation requests                   :0
  Rejected reassociation requests                     :0
  Failed reassociation requests                       :0
  Repeated reassociation requests                     :0
  Disassociations initiated by STAs                   :0
  Disassociations due to STA roaming                  :0
  Disassociations STAs go offline unexpectedly        :0
  Disassociations due to other reasons                :0
  Disassociations due to a link authentication failure :0
  Authentication requests                             :0
  Deauthentication requests                           :0
  STAs in power saving mode                           :0
  STAs in HT mode                                     :0
  STAs in B mode                                      :0
  STAs in G mode                                      :0
  STAs in A mode                                      :0
  STAs in N mode                                      :0
  STAs in AC mode                                     :0
  STAs in AX mode                                     :0
  STAs in BE mode                                     :0
  2.4G-only STAs                                      :0
  5G-only STAs                                        :0
  6G-only STAs                                        :0
  2.4G and 5G STAs                                    :0
  2.4G, 5G and 6G STAs                                :0
  2.4G and 5G STAs associated with 5G                 :0
  STAs associated with 2.4G band                      :0
  STAs associated with 5G band                        :0
  STAs associated with 6G band                        :0
  Band steer success rate(%)                          :-
```



```
Load balancing status between dual bands                :-
Sticky STAs detected                                    :0
--------------------------------------------------------------------------------
```

Table 11-57 Description of the **display station statistics ap-name** *ap-name* command output

Item	Description
Total online time of STAs (seconds)	Total online duration of all STAs, in seconds.
STAs associated with the AP	Number of STAs currently associated with the AP, not including the number of STAs in aging status.
Association requests	Number of association requests sent to the AP.
Successful association requests	Number of successful associations.
Rejected association requests	Number of association requests rejected by the AP.
Failed association requests	Number of failed associations.
Repeated association requests	Number of times STAs repeatedly send association requests to the AP.
Reassociation requests	Number of reassociation requests sent to the AP.
Successful reassociation requests	Number of successful reassociations.
Rejected reassociation requests	Number of reassociation requests rejected by the AP.
Failed reassociation requests	Number of failed reassociations.
Repeated reassociation requests	Number of times STAs repeatedly send reassociation requests to the AP.
Disassociations initiated by STAs	Number of times STAs are disassociated from the AP because users go offline.
Disassociations due to STA roaming	Number of times STAs are disassociated from the AP because users roam to other regions.
Disassociations because STAs go offline unexpectedly	Number of times STAs are disassociated from the AP because users go offline unexpectedly.
Disassociations due to other reasons	Number of times STAs are disassociated from the AP for other reasons.

Item	Description
Disassociations due to a link authentication failure	Number of times STAs are disassociated from the AP due to link authentication failures.
Authentication requests	Number of times link authentication requests are sent.
Deauthentication requests	Number of times link deauthentication requests are sent.
STAs in power saving mode	Number of STAs working in power saving mode.
STAs in HT mode	Number of STAs working in HT mode.
STAs in B mode	Number of STAs working in 802.11b mode.
STAs in G mode	Number of STAs working in 802.11g mode.
STAs in A mode	Number of STAs working in 802.11a mode.
STAs in N mode	Number of STAs working in 802.11n mode.
STAs in AC mode	Number of STAs working in 802.11ac mode.
STAs in AX mode	Number of STAs working in 802.11ax mode.
STAs in BE mode	Number of STAs working in 802.11be mode.
2.4G-only STAs	Number of STAs that support only the 2.4 GHz frequency band.
5G-only STAs	Number of STAs that support only the 5 GHz frequency band.
6G-only STAs	Number of STAs that support only the 6 GHz frequency band.
2.4G and 5G STAs	Number of STAs that support only the 2.4 GHz and 5 GHz frequency bands.
2.4G, 5G and 6G STAs	Number of STAs that support 2.4 GHz, 5 GHz, and 6 GHz frequency bands.
2.4G and 5G STAs associated with 5G	Number of STAs that support both 2.4 and 5 GHz frequency bands and are associated with the 5 GHz radio.

Item	Description
STAs associated with 2.4G band	Number of STAs associated with the 2.4 GHz radio.
STAs associated with 5G band	Number of STAs associated with the 5 GHz radio.
STAs associated with 6G band	Number of STAs associated with the 6 GHz radio.
Band steer success rate(%)	Band steering success rate.
Load balancing status between dual bands	Status of load balancing between different frequency bands.
Sticky STAs detected	Number of the detected sticky STAs.

11.1.91 display vap

Function

The **display vap** command displays information about service VAPs.

Format

display vap { **ap-group** *ap-group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] } [**ssid** *ssid*]

display vap { **all** | **ssid** *ssid* }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays information about all service VAPs in a specified AP group.	The AP group must exist.
ap-name *ap-name*	Displays information about service VAPs on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays information about service VAPs on the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Displays information about service VAPs on a specified radio.	The value is an integer that ranges from 0 to 2.
ssid *ssid*	Displays information about service VAPs with a specified SSID.	The SSID must exist.
all	Displays information about all service VAPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about service VAPs.

Example

Display information about all service VAPs.

```
<HUAWEI> display vap all
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name       RfID WID  BSSID          Status  Auth type  STA   SSID
--------------------------------------------------------------------------------
3     ap1           0    1    00e0-fc12-3456 ON      Open       0     GUEST-WLAN
--------------------------------------------------------------------------------
Total: 1
```

Table 11-58 Description of the **display vap** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
WID	WLAN ID of a VAP.
SSID	SSID name.
BSSID	MAC address of a VAP.
Status	Current status of a VAP. • ON: The VAP service is enabled. • OFF: The VAP service is disabled. • -: This is the state of a VAP on the standby AC in a dual-link cold backup scenario.
Auth type	Authentication mode of a VAP.
STA	Number of STAs connected to a VAP.

11.1.92 display vap create-fail-record

Function

The **display vap create-fail-record** command displays records about VAP creation failures.

Format

display vap create-fail-record { **ap-mac** *ap-mac* | **all** }

Parameters

Parameter	Description	Value
ap-mac *ap-mac*	Displays records about VAP creation failures on an AP with the specified MAC address.	The AP's MAC address must exist.
all	Displays records about VAP creation failures on all APs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vap create-fail-record** command to check records about VAP creation failures.

Example

Display all records about VAP creation failures.

```
<HUAWEI> display vap create-fail-record all
Rf/WLAN: Radio ID/WLAN ID
--------------------------------------------------------------------------------
AP MAC          Rf/WLAN  Profile Name  Source Type
VAP Type        Reason
--------------------------------------------------------------------------------
00e0-fc76-e360  0/4      1             ap-group
Service         Preshared key is not configured.
00e0-fc76-e370  1/4      1             ap-group
Service         Preshared key is not configured.
00e0-fc76-e360  0/6      1             ap-group
Service         Preshared key is not configured.
00e0-fc76-e370  1/6      1             ap-group
Service         Preshared key is not configured.
--------------------------------------------------------------------------------
Total records: 4
```


Table 11-59 Description of the **display vap create-fail-record all** command output

Item	Description
AP MAC	MAC address of an AP.
Rf/WLAN	Radio ID/WLAN ID.
Profile Name	VAP profile name.
Source Type	Object to which the VAP is bound, including: • ap-group: AP group • ap-id: AP
VAP Type	VAP type, including: • Service: Service VAP • WDS: WDS VAP • Mesh: Mesh VAP
Reason	Reason why the VAP fails to be created. **Table 11-60** describes detailed reasons.

Table 11-60 Reasons for VAP creation failures

Reason for VAP Creation Failures	Remarks	Suggestion
The VAPs using WEP encryption on an AP cannot use the same key ID.	-	Check the configuration of the VAP profile or security profile.
Invalid WEP key index.	-	Check whether the security profile is configured correctly.
Preshared key is not configured.	-	Configure a pre-shared key.
Only one management VAP profile can be bound.	-	Delete the management VAP that has been configured.
The bridge is enabled. Please undo first.	WLAN IDs 13 and 14 are used to set up a WDS bridge. Select other WLAN IDs or delete the WDS configuration.	Select another WLAN ID or delete the WDS configuration.

Reason for VAP Creation Failures	Remarks	Suggestion
WLAN ID(16) is used. Please undo first.	WLAN ID 16 is used to set up a Mesh link. Select another WLAN ID or delete the Mesh configuration.	Select another WLAN ID or delete the Mesh configuration.
Only one temporary management vap-profile can be bound to an AP.	-	Delete the offline management VAP that has been configured.
The current country code does not support 5GHz frequency band.	-	Change the country code, or do not create a 5 GHz VAP.
The current country code does not support 2.4GHz frequency band.	-	Change the country code, or do not create a 2.4 GHz VAP.
The AP type does not support the wlan id.	-	Delete unused VAPs.
This AP type does not support WDS function.	-	Replace the AP with one supporting WDS.
This AP type or version does not support Mesh function.	-	Replace the AP with a Mesh-capable AP or upgrade the AP to a Mesh-capable version.
The number of VAPs has reached the upper limit.	-	Delete excess VAPs.
The AP does not support 5GHz frequency band.	-	Change the AP, or do not create a 5 GHz VAP.
The AP does not support 2.4GHz frequency band.	-	Change the AP, or do not create a 2.4 GHz VAP.
The AP does not support 802.1X+WEP.	-	Replace the AP with one in compliance with 802.11ac Wave 2.
SFN roaming can be configured only on one VAP of each radio.	-	Create a VAP on another radio or delete the SFN roaming VAP on the current radio.
The AP does not support SFN.	-	Replace the AP with one supporting SFN roaming.

Reason for VAP Creation Failures	Remarks	Suggestion
The 5G radio of the AP does not support SFN. The radio frequency band of the AP does not support SFN.	-	Replace the AP or modify the radio configuration.
The number of VAPs has reached the card specific.	-	Reduce the number of VAPs on a card, or enable the AP to go online on another card of the switch and create VAPs.
The AP in this version does not support PPSK authentication.	-	Replace the AP with an AP that supports PPSK authentication or upgrade the AP to a version that supports PPSK authentication.
The AP in this version does not support the WPA3-Enterprise transition mode.	-	Upgrade the AP to V200R023C00 or later.
The AP in this version does not support Navi-AC VAPs.	-	Replace the AP with an AP that supports Navi AC VAPs or upgrade the AP to a version that supports Navi AC VAPs.
Unknown reason, error code is 0x%x.	-	Contact technical support personnel.
The number of WDS VAPs has reached the upper limit.	-	Delete redundant WDS VAPs.
The number of Mesh VAPs has reached the upper limit.	-	Delete redundant Mesh VAPs.
The frequency band of this radio is inconsistent with that supported by the current country code.	-	Change the country code, or do not create a VAP for the current radio.

Reason for VAP Creation Failures	Remarks	Suggestion
The AP in this version does not support the Mesh configuration on radio 2.	-	Replace the AP with an AP on which radio 2 supports Mesh or upgrade the AP to a version that supports Mesh on radio 2 of an AP.
The AP does not support OWE.	-	Replace the AP with an OWE-capable AP or upgrade the AP to an OWE-capable version.
No security policy is configured.	-	Configure a security policy.
No PSK is configured.	-	Configure a WEP key.
The 6GHz frequency band supports only the open, OWE and WPA3 security policies.	-	Modify the security policy configuration of the VAP.
The current country code does not support 6GHz frequency band.	-	Change the country code, or do not create a 6 GHz VAP.
The AP does not support 6GHz frequency band.	-	Change the AP, or do not create a 6 GHz VAP.
The 6G radio of the AP does not support SFN.	-	Replace the AP or modify the 6 GHz radio configuration.
The 6 GHz frequency band does not support WAPI, WPA, WPA2, and WEP.	-	Modify the encryption configuration of the VAP.
The AP in this version does not support RPSK authentication.	-	Replace the AP with an AP that supports RPSK authentication or upgrade the AP to a version that supports RPSK authentication.
The AP in this version does not support 802.1X +WPA3+AES.	-	Upgrade the AP to V200R023C00SPC100 or later.

11.1.93 display vap-profile

Function

The **display vap-profile** command displays configuration and reference information about VAP profiles.

Format

display vap-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all VAP profiles.	-
name *profile-name*	Displays information about a specified VAP profile.	The VAP profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check configuration and reference information about VAP profiles.

Example

Display information about all VAP profiles.

```
<HUAWEI> display vap-profile all
FMode   : Forward mode
STA U/D : Rate limit client up/down
VAP U/D : Rate limit VAP up/down
BR2G/5G/6G : Beacon 2.4G/5G/6G rate
-------------------------------------------------------------------------------------------------------------------
Name          FMode    Type     VLAN    AuthType  STA U/D(Kbps)  VAP U/D(Kbps)  BR2G/5G/6G(Mbps)
Reference  SSID
-------------------------------------------------------------------------------------------------------------------
default       direct   service  VLAN 1  Open      -/-            -/-            5.5/6/6          0         GUEST-WLAN
vap-profile1  direct   service  VLAN 1  Open      -/-            -/-            5.5/6/6          0         GUEST-WLAN
-------------------------------------------------------------------------------------------------------------------
Total: 2
```


Table 11-61 Description of the **display vap-profile all** command output

Item	Description
Name	VAP profile name.
FMode	Service data forwarding mode.
Type	VAP profile type. • service • management AP • service-backup ap-offline • service-backup auth-server-down • service-backup distribute
VLAN	Service VLAN ID.
AuthType	User authentication mode.
STA U/D(Kbps)	Uplink/downlink rate limit of a single STA.
VAP U/D(Kbps)	Uplink/downlink rate limit of all STAs on a specified VAP.
BR2G/5G/6G(Mbps)	Rate of Beacon frames on each frequency band.
Reference	Number of times a VAP profile is referenced.
SSID	SSID profile referenced by a VAP profile.

Display information about the VAP profile **default**.

```
<HUAWEI> display vap-profile name default
--------------------------------------------------------------------------------
Profile ID                          : 0
Service mode                        : enable
Type                                : service
Forward mode                        : direct-forward
Offline management                  : disable
Service VLAN ID                     : 1
Service VLAN Pool                   : -
Permit VLAN ID                      : 2 to 4
Auto off service switch             : disable
Auto off starttime                  : -
Auto off endtime                    : -
STA access mode                     : disable
STA blacklist profile               :
STA whitelist profile               :
Band steer                          : enable
Sta network detect                  : enable
Sta network detect(assoc)           : enable
Sta network detect(reassoc)         : enable
Learn client IPv4 address           : enable
Learn client DHCP strict            : disable
Learn client DHCP blacklist         : disable
Learn client IPv6 address           : enable
```



```
Learn client DHCPv6 strict                    : disable
Learn client DHCPv6 blacklist                 : disable
Learn client DHCPv6-SLAAC                     : disable
Learn client DHCPv6-SLAAC blacklist           : disable
IP source check                             : disable
ARP anti-attack check                         : disable
DHCP option82 insert                          : disable
DHCP option82 remote id format                : insert AP-MAC
  MAC format                                : default
DHCP option82 circuit id format               : insert AP-MAC
  MAC format                                : default
ND trust port                               : disable
SFN roam                                    : disable
Anti attack flood
  ARP flood switch                          : enable
  ARP flood STA rate threshold              : 4
  ARP flood blacklist                       : disable
  ND flood switch                           : enable
  ND flood STA rate threshold               : 8
  ND flood blacklist                        : disable
  IGMP flood switch                         : enable
  IGMP flood STA rate threshold             : 4
  IGMP flood blacklist                      : disable
  DHCP flood switch                         : enable
  DHCP flood STA rate threshold             : 4
  DHCP flood blacklist                      : disable
  DHCPv6 flood switch                       : enable
  DHCPv6 flood STA rate threshold           : 4
  DHCPv6 flood blacklist                    : disable
  mDNS flood switch                         : enable
  mDNS flood STA rate threshold             : 4
  mDNS flood blacklist                      : disable
  Other broadcast flood switch              : enable
  Other broadcast flood STA rate threshold  : 10
  Other broadcast flood blacklist           : disable
  Other multicast flood switch              : enable
  Other multicast flood STA rate threshold  : 10
  Other multicast flood blacklist           : disable
SSID profile                                : default
Security profile                            : default
Traffic profile                             : default
Authentication profile                      :
SAC profile                                 :
Hotspot2.0 profile                          :
Keep service                                : disable
Keep service allow new access               : disable
Keep service allow new access no auth       : disable
Service experience analysis                 : disable
SIP snooping port                           : 5060
mDNS Snooping switch                        : disable
MU BA Trigger mode                          : MU-BAR
Dynamic flow inspection switch              : enable
iConnect switch                             : disable
Split tunnel ACL                            :
User Flow syslog switch                     : enable
Multi-link operation                        : enable
Service experience analysis application list    :
------------------------------------------------------------------------------
Application ID    Application Name              UCL Group ID   UCL Group Name
------------------------------------------------------------------------------
------------------------------------------------------------------------------
S-IPFPM application list                    :
------------------------------------------------------------------------------
Application ID    Application Name              UCL Group ID   UCL Group Name
------------------------------------------------------------------------------
------------------------------------------------------------------------------
S-IPFPM flow list                           :
------------------------------------------------------------------------------
Flow ID    Role point    Direction    Bidirecion
```



```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
S-IPFPM clear color-flag ingress              : disable
--------------------------------------------------------------------------------
```

Table 11-62 Description of the **display vap-profile name** command output

Item	Description
Profile ID	VAP profile ID.
Service mode	Whether the VAP service is enabled. To configure this parameter, run the **service-mode disable** command.
Type	VAP type. ● service: service type ● ap-management: management AP type ● ap-offline: AP-offline backup service type ● service-backup distribute: distributed-AP backup service type To configure this parameter, run the **type (VAP profile view)** command.
Forward mode	Service data forwarding mode. ● direct-forward: direct forwarding ● tunnel: tunnel forwarding ● Soft-GRE: soft GRE forwarding To configure this parameter, run the **forward-mode** command.
Split tunnel ACL	Split tunneling ACL number. In this manner, packets matching the ACL rules can be forwarded in direct mode when the tunnel forwarding mode is configured. To configure this parameter, run the **split-tunnel** command.
Offline management	Whether the offline management VAP and antenna alignment VAP are enabled. To configure this parameter, run the **temporary-management enable (VAP profile view)** command.
Service VLAN ID	Service VLAN ID. To configure this parameter, run the **service-vlan (VAP profile view)** command.

Item	Description
Service VLAN Pool	VLAN pool to which a service VLAN belongs. To configure this parameter, run the **service-vlan (VAP profile view)** command.
Permit VLAN ID	VLAN from which packets are allowed to pass through when the authorization VLAN verification function is enabled.
Auto off service switch	Whether the scheduled VAP auto-off function is enabled. To configure this parameter, run the **auto-off service** command.
Auto off starttime	Start time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Auto off endtime	End time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Auto off track link	Whether to automatically disable VAPs upon disconnection of the uplink of a cloud AP. After this function is enabled through the iMaster NCE-Campus, the SSID is automatically disabled when the uplink of the cloud AP is disconnected. Only cloud APs support this parameter.
STA access mode	STA access control mode. To configure this parameter, run the **sta-access-mode** command.
STA blacklist profile	STA blacklist profile. To configure this parameter, run the **sta-access-mode** command.
STA whitelist profile	STA whitelist profile. To configure this parameter, run the **sta-access-mode** command.
Keep service	Whether service holding upon CAPWAP link disconnection is enabled. To configure this parameter, run the **keep-service enable (VAP profile view)** command.

Item	Description
Keep service allow new access	Whether new STAs are allowed to go online when APs are offline. To configure this parameter, run the **keep-service enable (VAP profile view)** command.
Keep service allow new access no auth	Whether offline APs allow Portal or MAC address authentication STAs to go online without authentication. To configure this parameter, run the **keep-service enable (VAP profile view)** command.
Band steer	Whether the band steering function is enabled. To configure this parameter, run the **band-steer disable** command.
Sta network detect(reassoc)	Whether network detection upon STA reassociation is enabled. To configure this parameter, run the **sta-network-detect disable** command.
Sta network detect(assoc)	Whether network detection upon STA association is enabled. To configure this parameter, run the **sta-network-detect assoc enable** command.
Learn client IPv4 address	Whether STA IPv4 address learning is enabled. To configure this parameter, run the **learn-client-address disable (VAP profile view)** command.
Learn client DHCP strict	Whether strict STA IP address learning through DHCP is enabled. To configure this parameter, run the **learn-client-address dhcp-strict** command.
Learn client DHCP blacklist	Whether to add STAs with bogus IP addresses to a dynamic blacklist. To configure this parameter, run the **learn-client-address dhcp-strict** command.

Item	Description
Learn client IPv6 address	Whether STA IPv6 address learning is enabled. To configure this parameter, run the **learn-client-address disable (VAP profile view)** command.
Learn client DHCPv6 strict	Whether strict STA IP address learning through DHCPv6 is enabled. To configure this parameter, run the **learn-client-address dhcpv6-strict** command.
Learn client DHCPv6 blacklist	Whether to add STAs with bogus IPv6 addresses to a dynamic blacklist. To configure this parameter, run the **learn-client-address dhcpv6-strict** command.
Learn client DHCPv6 SLAAC	Whether STA IPv6 address learning only through DHCPv6 or SLAAC is enabled. To configure this parameter, run the **learn-client-address dhcpv6-slaac** command.
Learn client DHCPv6 SLAAC blacklist	Whether to add STAs with bogus IPv6 addresses to a dynamic blacklist. To configure this parameter, run the **learn-client-address dhcpv6-slaac** command.
IP source check	Whether IPSG is enabled. To configure this parameter, run the **ip source check user-bind enable** command.
ARP anti-attack check	Whether DAI is enabled. To configure this parameter, run the **arp anti-attack check user-bind enable** command.
DHCP option82 insert	Whether to enable APs to add the Option 82 field to DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 insert enable** command.

Item	Description
DHCP option82 remote id format	Format of the remote-ID in the Option 82 field added to DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 format (VAP profile view)** command.
DHCP option82 circuit id format	Format of the circuit-ID in the Option 82 field added to DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 format (VAP profile view)** command.
MAC format	Format of the AP MAC address in the Option 82 field. To configure this parameter, run the **dhcp option82 format (VAP profile view)** command.
DHCP option82 remote id pattern	Field separator of remote-id suboptions for Option 82 in DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 pattern (VAP profile view)** command.
DHCP option82 circuit id pattern	Field separator of circuit-id suboptions for Option 82 in DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 pattern (VAP profile view)** command.
User defined text	User-defined format of Option 82's suboptions in DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 format (VAP profile view)** command.
ND trust port	Whether the ND trusted interface function is enabled. To configure this parameter, run the **nd trust port** command.
SFN roam	Whether agile distributed SFN roaming is enabled. To configure this parameter, run the **sfn-roam enable** command.

Item	Description
Anti attack flood	Flood detection and prevention.
ARP flood switch	Whether ARP flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
ARP flood STA rate threshold	Rate threshold for ARP flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
ARP flood blacklist	Whether the ARP flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
ND flood switch	Whether ND flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
ND flood STA rate threshold	Rate threshold for ND flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
ND flood blacklist	Whether the ND flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.

Item	Description
IGMP flood switch	Whether IGMP flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
IGMP flood STA rate threshold	Rate threshold for IGMP flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
IGMP flood blacklist	Whether the IGMP flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
DHCP flood switch	Whether DHCP flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
DHCP flood STA rate threshold	Rate threshold for DHCP flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
DHCP flood blacklist	Whether the DHCP flood blacklist function is enabled. To configure this parameter, run the **anti-attack flood blacklist enable** command. ● enable ● disable

Item	Description
DHCPv6 flood switch	Whether DHCPv6 flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
DHCPv6 flood STA rate threshold	Rate threshold for DHCPv6 flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
DHCPv6 flood blacklist	Whether the DHCPv6 flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
mDNS flood switch	Whether mDNS flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
mDNS flood STA rate threshold	Rate threshold for mDNS flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
mDNS flood blacklist	Whether the mDNS flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.

Item	Description
Other broadcast flood switch	Whether the flood detection function is enabled for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
Other broadcast flood STA rate threshold	Rate threshold for flood detection of broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
Other broadcast flood blacklist	Whether the flood blacklist function is enabled for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
Other multicast flood switch	Whether the flood detection function is enabled for multicast packets other than IGMP and mDNS packets. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
Other multicast flood STA rate threshold	Rate threshold for flood detection of multicast packets other than IGMP and mDNS packets. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.

Item	Description
Other multicast flood blacklist	Whether the flood blacklist function is enabled for multicast packets other than IGMP and mDNS packets. • enable • disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
SSID profile	Name of the SSID profile referenced by a VAP profile. To configure this parameter, run the **ssid-profile (VAP profile view)** command.
Security profile	Name of the security profile referenced by a VAP profile. To configure this parameter, run the **security-profile (VAP profile view)** command.
Traffic profile	Name of the traffic profile referenced by a VAP profile. To configure this parameter, run the **traffic-profile (VAP profile view)** command.
Authentication profile	Name of the authentication profile referenced by a VAP profile.
SAC profile	Name of the SAC profile referenced by a VAP profile. To configure this parameter, run the **sac-profile (VAP profile view)** command.
Hotspot2.0 profile	Name of the Hotspot2.0 profile referenced by a VAP profile. To configure this parameter, run the **hotspot2-profile (VAP profile view)** command.
SoftGRE profile	Name of the soft GRE profile referenced by a VAP profile. To configure this parameter, run the **forward-mode softgre** *profile-name* command.

Item	Description
Service experience analysis	Whether the SEA function is enabled. To configure this parameter, run the **service-experience-analysis enable** command.
SIP snooping port	SIP listening port number. To configure this parameter, run the **service-experience-analysis sip-snooping port** command.
mDNS Snooping switch	Whether the mDNS snooping function is enabled. To configure this parameter, run the **mdns-snooping enable** command.
MU BA Trigger mode	Mode in which STAs reply with Block Ack frames. To configure this parameter, run the **mu-ba-trigger mode** command.
Dynamic flow inspection switch	Whether the DFI function is enabled. To configure this parameter, run the **dynamic flow inspection enable** command.
iConnect	Whether the iConnect SSID is enabled. To configure this parameter, run the **iconnect enable** command.
User Flow syslog switch	Whether the function of sending network access flow logs of users to a log server is enabled.
Multi-link operation	Whether the MLO function is enabled. To configure this parameter, run the **mlo disable** command.
Service experience analysis application list	List of applications monitored based on SEA on the VAP. • Application ID • Application Name To configure this parameter, run the **service-experience-analysis monitor application** command.

Item	Description
S-IPFPM application list	List of applications on the VAP for which iPCA 2.0 measurement is performed. • Application ID • Application Name To configure this parameter, run the **s-ipfpm measure application** command.
S-IPFPM flow list	iPCA 2.0 flow measurement configuration on VAPs. • Flow ID: indicates the ID of a measurement flow. • Role point: indicates the role of a measurement point. • Direction: indicates the measurement flow direction. • Bidirecion: indicates whether a measurement flow is bidirectional. To configure this parameter, run the **s-ipfpm measure flow (VAP profile view)** command.
S-IPFPM clear color-flag ingress	Whether the function of clearing the color bit in the ingress direction on the edge node is enabled. • enable • disable To configure this parameter, run the **s-ipfpm clear color-flag ingress** command.

11.1.94 display vap-service-backup auth-server-down

Function

The **display vap-service-backup auth-server-down** command displays the status of an authentication-server-down backup service VAP.

Format

display vap-service-backup auth-server-down [**vap-profile** *profile-name*]

Parameters

Parameter	Description	Value
vap-profile *profile-name*	Specifies the name of a VAP profile.	The VAP profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the status of an authentication-server-down backup service VAP.

Example

Display the status of an authentication-server-down backup service VAP.

```
<HUAWEI> display vap-service-backup auth-server-down
-------------------------------------------------------------------------------------------
Vap-profile     VapSwitch      Mode      Radius-template     RadiusState
-------------------------------------------------------------------------------------------
vap-1           ON             Auto      Radius-1            Down
vap-2           ON             Manual    Radius-2            Down
vap-3           OFF            Manual    Radius-3            Up
-------------------------------------------------------------------------------------------
Total:3
```

Table 11-63 Description of the **display vap-service-backup auth-server-down** command output

Item	Description
Vap-profile	Name of a VAP profile.
VapSwitch	Status of the authentication-server-down backup service VAP.
Mode	Trigger mode of the authentication-server-down backup service VAP.
Radius-template	Name of a RADIUS server template.
RadiusState	Status of the RADIUS server.

11.1.95 display wlan config-errors

Function

The **display wlan config-errors** command displays WLAN configuration errors.

Format

display wlan config-errors

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check WLAN configuration errors.

Example

Display WLAN configuration errors.

```
<HUAWEI> display wlan config-errors
--------------------------------------------------------------------------------
Profile                                  Error
--------------------------------------------------------------------------------
vap-profile 1                            The authentication type specifie
d in the authentication-profile 1 does not match that in the security-profile 1.
--------------------------------------------------------------------------------
Total: 1
```

Table 11-64 Description of the **display wlan config-errors** command output

Item	Description
Profile	Profile name.
Error	Cause of a configuration error.

11.1.96 dot11a basic-rate

Function

The **dot11a basic-rate** command configures a basic rate set of the 802.11a protocol in a 5G radio profile.

The **undo dot11a basic-rate** command restores the default basic rate set of the 802.11a protocol in a 5G radio profile.

By default, a basic rate set of the 802.11a protocol in a 5G radio profile includes rates 6 Mbit/s, 12 Mbit/s, and 24 Mbit/s.

Format

dot11a basic-rate { *dot11a-rate-value* &<1-8> | **all** }

undo dot11a basic-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies a basic rate set.	The value is of the enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Supports all basic rates.	-

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The basic rate set includes all rates supported by both the AP and STA. A STA can associate with an AP only when the AP and STA support all rates in the basic rate set. For example, if you configure the basic rate set to contain rates 6 Mbit/s and 9 Mbit/s and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command to configure a basic rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11a

mode, the STA must support all rates specified by the basic rate set; otherwise, the STA cannot associate with the AP.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11a basic rate set to contain rates 6 Mbit/s and 9 Mbit/s in the 5G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] dot11a basic-rate 6 9
```

11.1.97 dot11a basic-rate (SSID profile view)

Function

The **dot11a basic-rate** command configures a basic rate set of the 802.11a protocol in an SSID profile.

The **undo dot11a basic-rate** command restores the default basic rate set of the 802.11a protocol in an SSID profile.

By default, no basic rate set of the 802.11a protocol is configured in an SSID profile, and the configuration in the radio profile takes effect.

NOTE

Only the AirEngine series APs support this command.

Format

dot11a basic-rate { *dot11a-rate-value* &<1-12> | **all** }

undo dot11a basic-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies a basic rate set.	The value is of the enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Supports all basic rates.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The basic rate set includes all rates supported by both the AP and STA. A STA can associate with an AP only when the AP and STA support all rates in the basic rate set. For example, if you configure the basic rate set to contain rates 6 Mbit/s and 9 Mbit/s and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command in an SSID profile to configure a basic rate set, bind the SSID profile to a VAP profile. If a STA associates with an AP in 802.11a mode, the STA must support all the rates in the basic rate set.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11a basic rate set to contain rates 6 Mbit/s and 9 Mbit/s in the SSID profile **default**

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] dot11a basic-rate 6 9
```

11.1.98 dot11a supported-rate

Function

The **dot11a supported-rate** command configures a supported rate set of the 802.11a protocol in a 5G radio profile.

The **undo dot11a supported-rate** command restores the default supported rate set of the 802.11a protocol in a 5G radio profile.

By default, the supported rate set of the 802.11a protocol in a 5G radio profile includes rates 6 Mbit/s, 9 Mbit/s, 12 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s, and 54 Mbit/s.

Format

dot11a supported-rate { *dot11a-rate-value* &<1-8> | **all** }

undo dot11a supported-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies a supported rate set.	The value is of the enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Supports all supported rates.	-

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP in addition to the basic rates. The AP and STA can transmit data at all rates specified in the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command to configure a supported rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11a mode, the AP and STA select a rate from the basic rate set or supported rate set to transmit packets.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11a supported rate set to contain rates 6 Mbit/s and 9 Mbit/s in the 5G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] dot11a supported-rate 6 9
```

11.1.99 dot11a supported-rate (SSID profile view)

Function

The **dot11a supported-rate** command configures a supported rate set of the 802.11a protocol in an SSID profile.

The **undo dot11a supported-rate** command restores the default supported rate set of the 802.11a protocol in an SSID profile.

By default, no supported rate set of the 802.11a protocol is configured in an SSID profile, and the configuration in the radio profile takes effect.

NOTE

Only the AirEngine series APs support this command.

Format

dot11a supported-rate { *dot11a-rate-value* &<1-12> | **all** }

undo dot11a supported-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies a supported rate set.	The value is of the enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Supports all supported rates.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP in addition to the basic rates. The AP and STA can transmit data at all rates specified in the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the

basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command in an SSID profile to configure a supported rate set, bind the SSID profile to a VAP profile. If a STA associates with an AP in 802.11a mode, the actual data transmission rate between the AP and STA is selected from the basic rate set and the rate set supported by the STA.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11a supported rate set to contain rates 6 Mbit/s and 9 Mbit/s in the SSID profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] dot11a supported-rate 6 9
```

11.1.100 dot11bg basic-rate

Function

The **dot11bg basic-rate** command configures a basic rate set of the 802.11b/g protocol in a 2G radio profile.

The **undo dot11bg basic-rate** command restores the default basic rate set of the 802.11b/g protocol in a 2G radio profile.

By default, the basic rate set of the 802.11b/g protocol includes rates 1 Mbit/s and 2 Mbit/s in a 2G radio profile.

Format

dot11bg basic-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg basic-rate

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies a basic rate set.	The value is of the enumerated type: • 1: 1 Mbit/s • 2: 2 Mbit/s • 5: 5.5 Mbit/s • 6: 6 Mbit/s • 9: 9 Mbit/s • 11: 11 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Supports all basic rates.	-

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The basic rate set includes all rates supported by both the AP and STA. A STA can associate with an AP only when the AP and STA support all rates in the basic rate set. For example, if you configure the basic rate set to contain rates 6 Mbit/s and 9 Mbit/s and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command to configure a basic rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11b/g mode, the STA must support all rates specified by the basic rate set; otherwise, the STA cannot associate with the AP.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11b/g mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11b/g basic rate set to contain rates 6 Mbit/s and 9 Mbit/s in the 2G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] dot11bg basic-rate 6 9
```

11.1.101 dot11bg basic-rate (SSID profile view)

Function

The **dot11bg basic-rate** command configures a basic rate set of the 802.11b/g protocol in an SSID profile.

The **undo dot11bg basic-rate** command restores the default basic rate set of the 802.11b/g protocol in an SSID profile.

By default, no basic rate set of the 802.11b/g protocol is configured in an SSID profile, and the configuration in the radio profile takes effect.

NOTE

Only the AirEngine series APs support this command.

Format

dot11bg basic-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg basic-rate

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies a basic rate set.	The value is of the enumerated type: • 1: 1 Mbit/s • 2: 2 Mbit/s • 5: 5.5 Mbit/s • 6: 6 Mbit/s • 9: 9 Mbit/s • 11: 11 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Supports all basic rates.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The basic rate set includes all rates supported by both the AP and STA. A STA can associate with an AP only when the AP and STA support all rates in the basic rate set. For example, if you configure the basic rate set to contain rates 6 Mbit/s and 9 Mbit/s and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command in an SSID profile to configure a basic rate set, bind the SSID profile to a VAP profile. If a STA associates with an AP in 802.11b/g mode, the STA must support all the rates in the basic rate set.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11b/g mode but does not take effect on STAs associated with the AP in other modes.

When the radio mode is 802.11b, only rates 1, 2, 5, and 11 Mbit/s take effect in the rate set configured in an SSID profile. If no rate in this rate set is configured in the SSID profile, the rate set configured in the radio profile is used.

Example

Configure the 802.11b/g basic rate set to contain rates 6 Mbit/s and 9 Mbit/s in the SSID profile **default**

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] dot11bg basic-rate 6 9
```

11.1.102 dot11bg supported-rate

Function

The **dot11bg supported-rate** command configures a supported rate set of the 802.11b/g protocol in a 2G radio profile.

The **undo dot11bg supported-rate** command restores the default supported rate set of the 802.11b/g protocol in a 2G radio profile.

By default, the supported rate set of the 802.11b/g protocol in a 2G radio profile includes rates 1 Mbit/s, 2 Mbit/s, 5.5 Mbit/s, 6 Mbit/s, 9 Mbit/s, 11 Mbit/s, 12 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s, and 54 Mbit/s.

Format

dot11bg supported-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg supported-rate

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies a supported rate set.	The value is of the enumerated type: • 1: 1 Mbit/s • 2: 2 Mbit/s • 5: 5.5 Mbit/s • 6: 6 Mbit/s • 9: 9 Mbit/s • 11: 11 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Supports all supported rates.	-

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP in addition to the basic rates. The AP and STA can transmit data at all rates specified in the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command to configure a supported rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11b/g mode, the AP and STA select a rate from the basic rate set or supported rate set to transmit packets.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11b/g mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11b/g supported rate set to contain rates 6 Mbit/s and 9 Mbit/s in the 2G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] dot11bg supported-rate 6 9
```

11.1.103 dot11bg supported-rate (SSID profile view)

Function

The **dot11bg supported-rate** command configures a supported rate set of the 802.11b/g protocol in an SSID profile.

The **undo dot11bg supported-rate** command restores the default supported rate set of the 802.11b/g protocol in an SSID profile.

By default, no supported rate set of the 802.11b/g protocol is configured in an SSID profile, and the configuration in the radio profile takes effect.

NOTE

Only the AirEngine series APs support this command.

Format

dot11bg supported-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg supported-rate

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies a supported rate set.	The value is of the enumerated type: • 1: 1 Mbit/s • 2: 2 Mbit/s • 5: 5.5 Mbit/s • 6: 6 Mbit/s • 9: 9 Mbit/s • 11: 11 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Indicates all supported rate sets.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP in addition to the basic rates. The AP and STA can transmit data at all rates specified in the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command in an SSID profile to configure a supported rate set, bind the SSID profile to a VAP profile. If a STA associates with an AP in 802.11b/g mode, the actual data transmission rate between the AP and STA is selected from the basic rate set and the rate set supported by the STA.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11b/g mode but does not take effect on STAs associated with the AP in other modes.

When the radio mode is 802.11b, only rates 1, 2, 5, and 11 Mbit/s take effect in the rate set configured in an SSID profile. If no rate in this rate set is configured in the SSID profile, the rate set configured in the radio profile is used.

Example

Configure the 802.11b/g supported rate set to contain rates 6 Mbit/s and 9 Mbit/s in the SSID profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] dot11bg supported-rate 6 9
```

11.1.104 dtim-interval

Function

The **dtim-interval** command sets the delivery traffic indication map (DTIM) interval in an SSID profile.

The **undo dtim-interval** command restores the default DTIM interval in an SSID profile.

By default, the DTIM interval is 1.

Format

dtim-interval *dtim-interval*

undo dtim-interval

Parameters

Parameter	Description	Value
dtim-interval	Specifies the DTIM interval.	The value is an integer that ranges from 1 to 255, in Beacons.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

DTIM refers to delivery traffic indication map. After a STA enters the dormancy mode, the associated AP saves the broadcast and multicast frames for the STA. When a Beacon frame sent to the STA by the AP contains DTIM, the saved broadcast and multicast frames will be transmitted to the STA. The DTIM interval refers to the number of Beacon frames sent before the Beacon frame that contains the DTIM. To set the interval for sending Beacon frames in an SSID profile, run the **beacon-interval** command.

- When the STA is in the dormancy status, the AP saves data transmitted to the STA and notifies the STA with a bit in broadcast Beacon frames. The STA receives data according to this bit. You can run this command to set the DTIM interval in the specified SSID profile.
- The DTIM interval specifies how many Beacon frames are sent before the Beacon frame that contains the DTIM. A long DTIM interval lengthens the dormancy time of the STA and saves power, but degrades the transmission capability of the STA. A short interval helps transmitting data in a timely manner, but the STA is woken up frequently, causing high power consumption.

Precautions

Changing the DTIM interval will restart the VAP to make the configuration take effect. During the VAP restart, services on the VAP are interrupted and STAs are disconnected.

Example

Set the DTIM interval to 5 in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dtim-interval 5
```

11.1.105 eirp

Function

(AP group radio view) The **eirp** command configures the transmit power for all specified radios in an AP group.

(AP group radio view) The **undo eirp** command restores the default transmit power for all specified radios in an AP group.

(AP radio view) The **eirp** command configures the transmit power for an AP radio.

(AP radio view) The **undo eirp** command cancels the configuration of the transmit power on an AP radio. The transmit power on the AP radio is then determined by that configured in the AP group radio view.

By default, the transmit power of a radio is 127 dBm. The transmit power that takes effect on APs is related to the AP type, country code, channel, and channel bandwidth. The transmit power in effect is the maximum transmit power that the AP radio supports under the current configuration. To check this value, run the **display radio** { **ap-name** *ap-name* | **ap-id** *ap-id* } command.

Format

eirp *eirp*

undo eirp

Parameters

Parameter	Description	Value
eirp	Specifies the transmit power.	The value is an integer that ranges from 1 to 127, in dBm.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Effective isotropic radiated power (EIRP) signifies the strength of signals transmitted from an antenna, that is, the transmit power of a radio plus the antenna gain. The transmit power of a radio configured using the **eirp** command is the EIRP plus the antenna gain on the radio.

You can configure the transmit power for a radio based on actual network environments, enabling radios to provide the required signal strength and improving signal quality on WLANs.

Precautions

The value of *antenna-gain* in the **antenna-gain** *antenna-gain* command must be consistent with the gain of the antenna connected to an AP.

If automatic transmit power selection is enabled by running the **calibrate auto-txpower-select enable** command, the transmit power configured by running the

eirp command does not take effect. The automatically selected transmit power is used.

If automatic transmit power selection is disabled by running the **calibrate auto-txpower-select disable** command, the transmit power configured by running the **eirp** command takes effect as follows:

The actual transmit power of an AP radio is determined by the configured transmit power of the radio, requirements of local laws and regulations, as well as the transmit power range supported by the AP. The actual transmit power of a radio cannot exceed the maximum transmit power required by local laws and regulations.

- If the configured transmit power of a radio is in compliance with local laws and regulations and within the transmit power range supported by the AP, the configured transmit power is the actual transmit power of the radio.
- If the configured transmit power of a radio is smaller than the minimum transmit power supported by the AP, the smaller one between the minimum transmit power supported by the AP and maximum transmit power required by local laws and regulations is the actual transmit power of the radio.
- If the configured transmit power of a radio is larger than the maximum transmit power supported by the AP, the smaller one between the maximum transmit power supported by the AP and maximum transmit power required by local laws and regulations is the actual transmit power of the radio.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Example

Set the transmit power of radio 0 on AP 1 to 30 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] eirp 30
Info: The EIRP value takes effect only when automatic transmit power selection i
s disabled, and the value depends on the AP specifications and local laws and re
gulations.
```

11.1.106 er-su disable

Function

The **er-su disable** command disables the Extended Range Single User (ER-SU) function.

The **undo er-su disable** command enables the ER-SU function.

By default, the ER-SU function is enabled.

NOTE

This command is not supported by the following models.

- AirEngine x760 series APs.

Format

er-su disable

undo er-su disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

The ER-SU function improves the signal quality at the cell edge and further improves the long-distance coverage capability.

Example

Disable the ER-SU function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan view] ssid-prof name test
[HUAWEI-wlan-ssid-prof-test] er-su disable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.107 forward-mode

Function

The **forward-mode** command sets the data forwarding mode in a VAP profile.

The **undo forward-mode** command restores the default data forwarding mode in a VAP profile.

By default, the direct forwarding mode is used in a VAP profile.

Format

forward-mode { **direct-forward** | **tunnel** | **softgre** *profile-name* }

undo forward-mode

Parameters

Parameter	Description	Value
direct-forward	Indicates the direct forwarding mode.	-
tunnel	Indicates the tunnel forwarding mode.	-
softgre *profile-name*	Indicates the soft GRE forwarding mode and specifies the name of the soft GRE profile bound to a VAP profile.	The specified soft GRE profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the forwarding mode in a VAP profile. The forwarding modes of each VAP profile can be different.

A soft GRE profile can be bound to a VAP profile only after the destination IP address of the soft GRE tunnel is configured in the soft GRE profile.

Example

Create the VAP profile **vap1** and set the forwarding mode to direct forwarding in the profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] forward-mode direct-forward
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.108 fragmentation-threshold

Function

The **fragmentation-threshold** command sets the fragmentation threshold in a radio profile.

The **undo fragmentation-threshold** command restores the default fragmentation threshold in a radio profile.

By default, the packet fragmentation threshold is 2346 bytes.

Format

fragmentation-threshold *fragmentation-threshold*

undo fragmentation-threshold

Parameters

Parameter	Description	Value
fragmentation-threshold	Specifies the fragment threshold. If the length of a frame to be sent by the MAC layer exceeds this threshold, the frame is fragmented before being sent.	The value is an integer that ranges from 256 to 2346, in bytes. It must be an integral multiple of 2.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A proper packet fragmentation threshold can improve channel bandwidth usage. Set the fragmentation threshold as required. A large threshold is recommended.

Precautions

When the packet fragmentation threshold is too small, packets are fragmented into smaller frames. These frames are transmitted at a high extra cost, resulting in low channel efficiency.

When the packet fragmentation threshold is too large, long packets are usually not fragmented, which increases the transmission time and error probability. If an error occurs, packets are retransmitted, resulting in a waste of channel bandwidth.

Example

Set the fragmentation threshold to 1500 bytes in the 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] fragmentation-threshold 1500
```


11.1.109 frequency

Function

(AP group radio view) The **frequency** command sets the working frequency band of radios for all APs in an AP group.

(AP group radio view) The **undo frequency** command restores the default working frequency band of radios for all APs in an AP group.

(AP radio view) The **frequency** command sets the working frequency band of radios for an AP.

(AP radio view) The **undo frequency** command restores the default working frequency band of the radio on an AP to that configured in the AP group radio view.

By default, radio 0 and radio 2 in the AP group radio view work on the 2.4 GHz and 6 GHz frequency bands, respectively. If radio 2 does not support the 6 GHz frequency band, it works on the frequency band by default. There is no default value in the AP radio view, and the configuration in the AP group radio view is used.

Format

frequency { **2.4g** | **5g** | **6g** }

undo frequency

Parameters

Parameter	Description	Value
2.4g	Specifies 2.4 GHz frequency band.	-
5g	Specifies 5 GHz frequency band.	-
6g	Specifies the 6 GHz frequency band.	-

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Radios of some AP models support frequency band switching but can work on only one frequency band at a time. You can configure the working frequency band of AP radios based on the frequency bands supported by STAs.

Precautions

When working in dual-5G mode, some APs support only low-band channels (36 to 64) or high-band channels (100 to 165) on the 5 GHz band.

- AirEngine 5760-51: Radio 1 on high bands and radio 2 on low bands
- AirEngine 6760-X1: Radio 1 on high bands and radio 2 on low bands
- AirEngine 6760-X1E: Radio 1 on high bands and radio 2 on low bands
- AirEngine 8760R-X1E: Radio 1 and radio 2 on all bands
- AirEngine 8760-X1-PRO: Radio 1 on high bands and radio 2 on low bands
- AirEngine 6761-21T: Radio 1 on high bands and radio 2 on low band
- AirEngine 6761S-21T: Radio 1 on high bands and radio 2 on low band
- AirEngine 5761R-11E: Radio 0 and radio 1 on all bands
- AirEngine 8771-X1T: Radio 1 on low bands and radio 2 on high band

Changing the working frequency band of radio 0 and radio 2 will delete the channel, power, and antenna gain configurations on radio 0 and radio 2. If an AP uses an external antenna, run the **antenna-gain** *antenna-gain* command to reconfigure the antenna gain to be consistent with the gain of the external antenna connected to the AP.

If the working frequency band of the AP radio set using the preceding commands is the same as that of the AP's actual working frequency band, the AP will not restart. Otherwise, the AP restarts after the preceding commands are run.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

If two radios of an AP work on the 5 GHz frequency band, the operating channels of the two 5 GHz radios must be separated by at least one channel to avoid interference. If two radios of an AP work on the 5 GHz and 6 GHz frequency bands, respectively, pay attention to channel planning as follows:

- For the model AirEngine 6761-22T: Do not use a 5 GHz high-frequency channel (149–165) and a 6 GHz low-frequency channel (80 MHz channels 1–13, 160 MHz channels 1–29) at the same time.
- For the model AirEngine 8771-X1T: Do not use a 5 GHz high-frequency channel (20 MHz channels 153–165, 40 MHz channels 132–161, 80 MHz channels 132–161, 160 MHz channels 100–128, 320 MHz channels 100–144) and a 6 GHz channel (160 MHz channels 1–29, 320 MHz channels 1–61) at the same time.

For example, a country supports 40 MHz+ 5G channels 36, 44, 52, and 60. When deploying 5 GHz radio channels, if one radio is deployed to work on channel 36, it is recommended that channel 52 or 60 be configured for the other radio. Channel 44 is not recommended in this case.

Example

Set the working frequency band of radio 0 of AP to the 5 GHz band.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] radio 0
[HUAWEI-wlan-radio-0/0] frequency 5g
Warning: Modifying the frequency band will delete the channel, power, and antenn
a gain configurations of the current radio on the AP and reboot the AP. Continue
?[Y/N]:Y
```

11.1.110 guard-interval-mode

Function

The **guard-interval-mode** command configures the guard interval (GI) mode.

The **undo guard-interval-mode** command restores the default GI mode.

By default, the GI mode in 802.11n/ac is **short**, and the GI mode in 802.11ax/be is 0.8 us.

Format

guard-interval-mode { **short** | **normal** }

undo guard-interval-mode

guard-interval-mode dot11ax { **dot8** | **1dot6** | **3dot2** }

undo guard-interval-mode dot11ax

Parameters

Parameter	Description	Value
short	Sets the GI mode in 802.11n/ac to short GI.	-
normal	Sets the GI mode in 802.11n/ac to normal GI.	-
dot11ax { **dot8** | **1dot6** | **3dot2** }	Specifies the GI mode in 802.11ax/be.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

During data transmission, the receive and transmit ends do not receive and send data at all times. When data is received and transmitted or multiple transmissions

occur, multi-path interference is generated in radio signal propagation. An interval between transmissions can reduce the impact of interference. This interval is called guard interval (GI).

A smaller GI indicates higher transmission efficiency. A larger GI indicates a higher anti-interference capability. A small GI is recommended for indoor areas with low interference, and a large GI is recommended for outdoor areas with high interference.

- In 802.11a/b/g, the GI is fixed at 800 ns.
- In 802.11n and 802.11ac, the GI can be set to 400 ns (short) or 800 ns (normal).
- In 802.11ax and 802.11be, the GI can be set to 0.8 us (800 ns), 1.6 us, or 3.2 us.

Example

Set the GI mode to short.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] guard-interval-mode short
```

11.1.111 he mcs-map (SSID Profile)

Function

The **he mcs-map** command configures the number of 802.11ax spatial streams and the Modulation and Coding Scheme (MCS) of the spatial streams in an SSID profile.

The **undo he mcs-map** command restores the default number of 802.11ax spatial streams and the default MCS of the spatial streams in an SSID profile.

By default, the number of spatial streams sent and received in 802.11ax is 8, and the MCS of the spatial streams is 11 in an SSID profile.

Format

he { **tx** | **rx** } **mcs-map nss** *nss-value* **map** *mcs-value*

undo he { **tx** | **rx** } **mcs-map**

Parameters

Parameter	Description	Value
tx	Indicates the sent data.	-
rx	Indicates the received data.	-
nss *nss-value*	Specifies the number of spatial streams.	The value is an integer that ranges from 1 to 8.

Parameter	Description	Value
map *mcs-value*	Specifies the MCS of the spatial streams.	The value can be 7, 9, or 11.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The rate of an 802.11ax-capable AP depends on the index value of the MCS. A larger MCS indicates a higher transmission rate.

- When the value of *nss-value* is greater than or equal to the number of spatial streams actually supported by an AP, the MCS value corresponding to all the spatial streams of the AP is the value of *mcs-value*.
- When the value of *nss-value* is smaller than the number of spatial streams actually supported by an AP, only the MCS value corresponding to the spatial streams on the AP is the value of *mcs-value*, and the maximum MCS value corresponding to other spatial streams does not take effect.

  For example, if the value of *nss-value* is 2, and the AP supports three spatial streams, only the MCS value corresponding to spatial streams 1 and 2 is the value of *mcs-value*, and the MCS value corresponding to spatial stream 3 does not take effect.

Precautions

This configuration takes effect only when the AP communicates with STAs through 802.11ax.

Example

Set the MCS value corresponding to spatial stream 4 to 9 when data is received in an SSID profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] he rx mcs-map nss 4 map 9
```

11.1.112 a-mpdu disable

Function

The **a-mpdu disable** command disables the aggregate MAC protocol data unit (A-MPDU) function.

The **undo a-mpdu disable** command enables the A-MPDU function.

By default, the A-MPDU function is enabled.

Format

a-mpdu disable

undo a-mpdu disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce costs, 802.11n uses A-MPDU technology that aggregates two or more MPDUs into one frame for transmission.

The 802.11ac and later protocols require that the A-MPDU mode be enabled. Therefore, this command takes effect only for 802.11n APs.

Example

Disable the A-MPDU function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] a-mpdu disable
```

11.1.113 ht a-mpdu max-length-exponent

Function

The **ht a-mpdu max-length-exponent** command sets the maximum length of an aggregated MPDU (A-MPDU) on the 802.11n radio. MPDU stands for MAC protocol data unit.

The **undo ht a-mpdu max-length-exponent** command restores the maximum length of an A-MPDU on the 802.11n radio to the default value.

By default, the index for the maximum length of an A-MPDU is 3. The maximum length of the A-MPDU is 65535 bytes.

The function is not supported by the following models.

- AirEngine series APs

Format

ht a-mpdu max-length-exponent *max-length-exponent-index*

undo ht a-mpdu max-length-exponent

Parameters

Parameter	Description	Value
max-length-exponent-index	Indicates the index for the maximum length of the A-MPDU.	The value is an integer that ranges from 0 to 3. ● 0: indicates that the maximum length of the A-MPDU is 8191 bytes. ● 1: indicates that the maximum length of the A-MPDU is 16383 bytes. ● 2: indicates that the maximum length of the A-MPDU is 32767 bytes. ● 3: indicates that the maximum length of the A-MPDU is 65535 bytes.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce costs, 802.11n uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

Set the index of the maximum length of the A-MPDU to 2 in the 2G radio profile **default**. The index 2 corresponds to a maximum length of 32767 bytes.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] ht a-mpdu max-length-exponent 2
```

11.1.114 keepalive (soft GRE profile view)

Function

The **keepalive** command enables Keepalive detection for a soft GRE tunnel and sets Keepalive parameters.

The **undo keepalive** command disables Keepalive detection for a soft GRE tunnel and restores the default Keepalive parameters.

By default, Keepalive detection is disabled for a soft GRE tunnel, the interval for sending Keepalive packets is 5 seconds, and the maximum number of retransmission attempts is 3.

Format

keepalive [**period** *period* [**retry-times** *retry-times*]]

undo keepalive

Parameters

Parameter	Description	Value
period *period*	Specifies the interval for sending Keepalive packets.	The value is an integer that ranges from 1 to 32767, in seconds.
retry-times *retry-times*	Specifies the maximum number of Keepalive packet retransmission times.	The value is an integer that ranges from 1 to 255.

Views

Soft GRE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a network fault occurs and the remote end of a soft GRE tunnel becomes unreachable, an AP cannot detect the network fault and therefore will continue to send packets to the remote end. These packets waste device resources and bandwidth of the intermediate network. After Keepalive detection for a soft GRE

tunnel is enabled, the AP can detect the soft GRE tunnel status. When detecting that the peer end of the soft GRE tunnel is unreachable, the AP stops sending packets to the peer end. Otherwise, the AP continues sending packets to the peer end. This mechanism reserves device resources and bandwidth.

After the Keepalive detection function for the soft GRE tunnel is enabled, the local AP periodically sends Keepalive packets to the peer end at specified intervals to check connectivity of the soft GRE tunnel. The value of the unreachable counter is incremented by 1 each time a Keepalive packet is sent but no response is received within the detection period. If a response is received before the value of **retry-times** is reached, the counter is reset. If the AP does not receive any response from the peer end when the counter value reaches the preset value (**retry-times**), it considers the peer unreachable and terminates the tunnel. If the AP receives a response, it considers the peer reachable and continues sending packets to the peer end.

Precautions

If only the **keepalive** command is executed and the parameter **period** *period* [**retry-times** *retry-times*] is not specified, the Keepalive detection function is enabled and the default value of **period** *period* [**retry-times** *retry-times*] parameter is used.

If you run the **keepalive** command several times, the latest configuration overrides the previous configurations.

The Keepalive detection function for a soft GRE tunnel takes effect unidirectionally. If the Keepalive detection function is required on both ends of a soft GRE tunnel, enable this function on each end of the tunnel. The Keepalive detection function takes effect on one end even if the function is disabled on the other end. However, you are advised to enable the Keepalive detection function on both ends of a tunnel.

Example

Enable the Keepalive detection function for a soft GRE tunnel using default parameters.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] softgre-profile name soft1
[HUAWEI-wlan-softgre-prof-soft1] keepalive
```

11.1.115 keep-service enable (VAP profile view)

Function

The **keep-service enable** command enables service holding upon CAPWAP link disconnection.

The **undo keep-service enable** command disables service holding upon CAPWAP link disconnection.

By default, service holding upon CAPWAP link disconnection is disabled.

Format

keep-service enable [**allow new-access** [**no-auth**]]

undo keep-service enable

Parameters

Parameter	Description	Value
allow new-access	Enables offline APs to allow access of new STAs.	-
no-auth	Allows STAs using Portal or MAC address authentication to go online without authentication.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In direct forwarding mode, you can enable service holding upon CAPWAP link disconnection. In this way, when the CAPWAP link between an AP and AC is disconnected, the AP can continue to provide WLAN services, preventing service interruption and improving forwarding reliability.

Service holding upon CAPWAP link disconnection controls whether new STAs are allowed to go online. For high-security authentication modes such as MAC address authentication and Portal authentication, **no-auth** must be configured to enable STAs to go online without authentication upon CAPWAP link disconnection. Therefore, this function can be enabled in scenarios with low security requirements.

Precautions

- Service holding upon CAPWAP link disconnection can be configured in the VAP profile view and AP system profile view. The configuration in the VAP profile view takes precedence over that in the AP system profile view.
- Service holding upon CAPWAP link disconnection is applicable only to scenarios where direct forwarding is used for data services.
- The function of enabling offline APs to allow access of STAs is applicable to scenarios where service data is forwarded in direct mode and the STA authentication mode is Portal, MAC address, WEP, WPA/WPA2-PSK, or open system.

- Service holding upon CAPWAP link disconnection cannot be configured together with the AP-offline backup service VAP (configured using the **type service-backup ap-offline** command) or containment function. Service holding upon CAPWAP link disconnection does not take effect when the containment function is also configured.
- Service holding upon CAPWAP link disconnection is unavailable on a WDS network.
- After service holding upon CAPWAP link disconnection is enabled, the **display access-user** command cannot display information about NAC STAs that are online before the CAPWAP link is disconnected. To display information about such STAs, run the **display station** command.

Example

Enable service holding upon CAPWAP link disconnection in the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] keep-service enable
```

11.1.116 legacy-station disable

Function

The **legacy-station disable** command denies access of non-HT STAs.

The **undo legacy-station disable** command permits access of non-HT STAs.

By default, access of non-HT STAs is permitted.

Format

legacy-station [**only-dot11b**] **disable**

undo legacy-station disable

Parameters

Parameter	Description	Value
only-dot11b	Denies access of non-HT STAs that support only 802.11b.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Non-HT STAs support only 802.11a/b/g and provide a data transmission rate far smaller than the rate of STAs in compliance with 802.11n or later standards. If the non-HT STAs access the WLAN, the data transmission rate of STAs in compliance with 802.11n or later standards will be reduced. To prevent the transmission rate of these STAs from being affected, you can run the **legacy-station** [**only-dot11b**] **disable** command to deny access of all or only 802.11b-compliant non-HT STAs.

Configuration Impact

After the **legacy-station disable** command is run, non-HT STAs supporting only 802.11a/b/g cannot access the wireless network.

After the **legacy-station only-dot11b disable** command is run, non-HT STAs supporting only 802.11b cannot access the wireless network.

After access of non-HT STAs is denied, services may be interrupted.

Precautions

After the **legacy-station disable** command is run, the access of non-HT STAs supporting only 802.11a/b/g fails to be denied if any of the following functions is configured on the non-HT STAs:

- WMM function in a 2G or 5G radio profile disabled using the **wmm disable** command
- Pre-shared key authentication and TKIP encryption for WPA/WPA2 configured using the **security** { **wpa** | **wpa2** | **wpa-wpa2** } **psk** { **pass-phrase** | **hex** } *key-value* **tkip** command when the security profile is used
- 802.1X authentication and TKIP encryption for WPA/WPA2 configured using the **security** { **wpa** | **wpa2** | **wpa-wpa2** } **dot1x tkip** command when the security profile is used
- WEP authentication configured using the **security wep** [**share-key** | **dynamic**] command when the security profile is used
- 802.11b/g radio type in the 2G radio profile configured using the **radio-type** { **dot11b** | **dot11g** } command
- 802.11a radio type in the 5G radio profile configured using **radio-type dot11a** command

After the **legacy-station only-dot11b disable** command is run, the access of non-HT STAs supporting only 802.11b is denied. If 802.11b radio type in the 2G radio profile has been configured using the **radio-type dot11b** command, the access of non-HT STAs supporting only 802.11b fails to be denied.

Example

Deny access of non-HT STAs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] legacy-station disable
Warning:  If the wmm disable command, TKIP, WEP, or radio type of 802.11a/b/g is configured, the function of denying access of legac
y STAs cannot take effect.
```


11.1.117 max-sta-number (SSID profile view)

Function

The **max-sta-number** command sets the maximum number of STAs that can be associated with a single VAP.

The **undo max-sta-number** command restores the default maximum number of STAs that can be associated with a single VAP.

By default, a VAP allows for association of a maximum of 64 STAs.

Format

max-sta-number *max-sta-number*

undo max-sta-number

Parameters

Parameter	Description	Value
max-sta-number	Specifies the maximum number of STAs that can be associated with a single VAP.	The value is an integer that ranges from 1 to 512.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

More access users on a VAP indicate fewer network resources that each user can occupy. To ensure Internet experience of users, you can run this command to properly set the maximum number of STAs that can be associated with a single VAP.

Configuration Impact

After this command is executed, online STAs are disconnected. When STAs reassociate with the VAP and the number of associated STAs on the VAP reaches the maximum, new STAs fail to associate with this VAP.

The **max-sta-number** *max-sta-number* command sets the maximum number of STAs that can be associated with a single VAP.

Precautions

The setting configured by this command refers to the maximum number of STAs that can be associated with a VAP of a single AP.

Example

Set the maximum number of STAs that can be associated with a single VAP to 50.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] max-sta-number 50
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.118 mlo enable

Function

The **mlo enable** command enables the multi-link operation (MLO) function.

The **mlo disable** command disables the MLO function.

The **undo mlo** command restores the default status of the MLO function.

By default, the MLO function is disabled.

Format

mlo { **enable** | **disable** }

undo mlo

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA communicates with an AP, the STA selects only one radio to set up a connection, for example, on the 2.4 GHz or 5 GHz frequency band. The maximum air interface rate of the STA is the maximum capability supported by the current radio. To further improve the air interface rate and reduce latency, 802.11be introduces the MLO function that allows for link setup on multiple radios for communication. To improve the air interface rate, transmit different data on different radios at the same time. Radios can back up each other so when the

channel is busy on a radio, data is quickly switched to another radio for transmission, reducing air interface latency.

Precautions

After the MLO function is enabled, some incompatible STAs may fail to detect Wi-Fi signals or fail to associate with the WLAN. Such issues can be resolved after you disable the MLO function.

Currently, an AP supports a maximum of two concurrent radios, for example, 2.4 GHz + 5 GHz radios or 5 GHz + 6 GHz radios.

Both the AP and the STA need to support the MLO function. If both the AP and STA support the MLO function on the 2.4 GHz, 5 GHz, and 6 GHz frequency bands, the high-speed 5 GHz + 6 GHz radios are used to set up a link between the AP and STA. If the STA supports the MLO function only on the 2.4 GHz and 5 GHz frequency bands, the link can be set up only using 2.4 GHz + 5 GHz radios.

After the MLO function is enabled, if the configuration of one radio is modified and the modification affects MLO link renegotiation, VAP services on the two radios are interrupted, causing STAs to go offline and online again. Services of other VAPs on the radios are not affected. The configurations that affect MLO link renegotiation include: whether MLO is enabled, radio type, whether the radio is enabled, binding relationship between the VAP profile and radio, security policy, and SSID name.

After an MLO link is set up, information about the STA connected to the device can be viewed only on one radio. However, traffic statistics about the STA are still collected on the two radios. To view information about the access radio of the STA, log in to the AP associated with the STA and run the **display umac station mac** *mac-address* command in the diagnostic view to display MLO link setup information about the STA.

The MLO function takes effect only when the following conditions are met:

- A VAP profile is bound to multiple radios of an AP, and the WLAN IDs of the radios are the same.
- The radios work in 802.11be mode.
- The security policy is open (only 2.4 GHz + 5 GHz radios supported), WPA2 (only 2.4 GHz + 5 GHz radios supported), WPA3, WPA2-WPA3 (only 2.4 GHz + 5 GHz radios supported), or OWE.

The MLO and 802.11r fast roaming functions are mutually exclusive. After the 802.11r fast roaming function is enabled, the MLO function does not take effect.

Example

Enable the MLO function in the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] mlo enable
Warning: After the MLO function is enabled, some incompatible STAs may fail to detect Wi-Fi signals and cannot associate with the WLAN. This issue can be resolved after you disable the MLO function.
Warning: This action may cause service interruption. Continue?[Y/N]y
```


11.1.119 mu-ba-trigger mode

Function

The **mu-ba-trigger mode** command sets the mode in which STAs reply with Block Ack frames.

The **undo mu-ba-trigger mode** command restores the default mode in which STAs reply with Block Ack frames.

By default, STAs reply with Block Ack frames in MU-BAR mode.

This command is supported on the following APs.

- AirEngine x761
- AirEngine x762
- AirEngine x771

Format

mu-ba-trigger mode { **basic-trigger** | **mu-bar** }

undo mu-ba-trigger mode

Parameters

Parameter	Description	Value
basic-trigger	A-MPDU with basic trigger	-
mu-bar	A-MPDU with MU-BAR	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

The **mu-ba-trigger mode** command sets the mode in which STAs reply with Block Ack frames.

Example

Set the mode in which STAs reply with Block Ack frames to basic-trigger.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-wlan-vap-prof-test] mu-ba-trigger mode basic-trigger
```


11.1.120 mu-mimo disable

Function

The **mu-mimo disable** command disables the downlink MU-MIMO scheduling function.

The **undo mu-mimo disable** command enables the downlink MU-MIMO scheduling function.

By default, the downlink MU-MIMO scheduling function is enabled.

Format

mu-mimo disable

undo mu-mimo disable

Parameters

None

Views

SSID profile view, WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Carrier sense multiple access with collision avoidance (CSMA-CA) allows an air interface channel to be occupied only by one STA, and other STAs cannot communicate with the AP. After downlink MU-MIMO scheduling is enabled, STAs supporting MU-MIMO can form an MU group to simultaneously receive downlink data from the same air interface channel, improving channel efficiency and overall downlink throughput.

Prerequisites

Before enabling downlink MU-MIMO scheduling, run the **undo beamforming disable** command to enable beamforming.

Precautions

- In WDS scenarios, ensure that the number of spatial streams on STA VAPs is smaller than that on AP VAPs. Otherwise, MU-MIMO cannot take effect. For example, if STA VAPs and AP VAPs are both configured with three spatial streams, an AP VAP can communicate with only one STA VAP even if MU-MIMO has been enabled.
- downlink MU-MIMO scheduling is not supported in the Mesh networking.

In VR scenarios, disabling downlink MU-MIMO scheduling is recommended.

Example

Enable in the SSID profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] undo mu-mimo disable
```

11.1.121 mu-mimo optimize enable

Function

The **mu-mimo optimize enable** command enables the MU-MIMO optimization function.

The **undo mu-mimo optimize enable** command disables the MU-MIMO optimization function.

By default, the MU-MIMO optimization function is disabled.

Format

mu-mimo optimize enable

undo mu-mimo optimize enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an environment with less interference, you can run the **mu-mimo optimize enable** command to enable the MU-MIMO optimization function to meet requirements for high downlink throughput of the AP. The expected effect may fail to be achieved in some scenarios.

Prerequisites

The MU-MIMO function has been enabled using the **undo mu-mimo disable** command.

NOTE

The MU-MIMO optimization function is not supported by the following models.

- AirEngine series APs

Example

Enable the MU-MIMO optimization function in the SSID profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] undo mu-mimo disable
[HUAWEI-wlan-ssid-prof-test] mu-mimo optimize enable
```

11.1.122 ofdma downlink disable

Function

The **ofdma downlink disable** command disables the downlink (DL) OFDMA function.

The **undo ofdma downlink disable** command enables the DL OFDMA function.

By default, the DL OFDMA function is enabled.

Format

ofdma downlink disable

undo ofdma downlink disable

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

OFDMA is a multi-user technology introduced in 802.11ax. This function improves the utilization of wireless spectrum resources, supports more concurrent STAs, and improves user experience in wireless Internet access.

Example

Enable the DL OFDMA function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] undo ofdma downlink disable
```

11.1.123 ofdma uplink disable

Function

The **ofdma uplink disable** command disables the uplink (UL) OFDMA function.

The **undo ofdma uplink disable** command enables the UL OFDMA function.

By default, the UL OFDMA function is enabled.

Format

ofdma uplink disable

undo ofdma uplink disable

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

OFDMA is a multi-user technology introduced in 802.11ax. This function improves the utilization of wireless spectrum resources, supports more concurrent STAs, and improves user experience in wireless Internet access.

Example

Enable the UL OFDMA function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] undo ofdma uplink disable
```

11.1.124 probe-response-retry

Function

The **probe-response-retry** command sets the number of times Probe Response packets are retransmitted.

The **undo probe-response-retry** command restores the default number of times Probe Response packets are retransmitted.

By default, the number of Probe Response retransmissions is 1.

Format

probe-response-retry *retry-time*

undo probe-response-retry

Parameters

Parameter	Description	Value
retry-time	Specifies the number of times Probe Response packets are retransmitted.	The value is an integer that ranges from 0 to 3. When the value is set to 0, Probe Response packets are not retransmitted.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many Probe Response frames occupy a large number of wireless resources. To reduce wireless resource occupation of the frames, you can run the **probe-response-retry** command to set a small number of or forbid Probe Response packet retransmissions.

Precautions

A small number of Probe Response packet retransmissions may reduce the channel scan efficiency of some STAs while a large number of Probe Response packet retransmissions may lower the wireless network performance.

Example

Set the number of times Probe Response packets are retransmitted to 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] probe-response-retry 0
```

11.1.125 qbss-load enable

Function

The **qbss-load enable** command enables the function of notifying STAs of AP load information.

The **undo qbss-load enable** command disables the function of notifying STAs of AP load information.

By default, the function of notifying STAs of AP load information is disabled.

Format

qbss-load enable

undo qbss-load enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

After the **qbss-load enable** command is executed, STAs are notified of the AP load status during the STA association. The notified information includes the number of STAs associated with AP radios and channel utilization. A STA selects the optimal AP based on the load of each AP to improve air interface performance.

NOTE

This command takes effect only when dynamic load balancing is disabled, because with dynamic load balancing enabled, APs will definitely notify STAs of their loads.

Modifying this configuration will cause STAs connected to the SSID to go offline and then online, interrupting STAs' services.

Example

Enable the function of notifying STAs of AP load information in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] qbss-load enable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.126 radio

Function

The **radio** command displays the radio view.

Format

radio *radio-id*

Parameters

Parameter	Description	Value
radio-id	Specifies the radio ID.	The radio ID must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The radio configuration in the AP group view or AP view takes effect on all radios at the same time. To configure only a specified radio, enter the view of the radio to configure its parameters.

Precautions

If you run this command in the AP group view, configurations on all specified radios in the AP group are allowed. If you run this command in the AP view, configurations only on the specified radio on the AP are allowed.

Example

Display the view of radio 0 on AP 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] radio 0
[HUAWEI-wlan-radio-0/0]
```

11.1.127 radio disable

Function

(AP group radio view) The **radio disable** command disables specified radios on all APs in an AP group.

(AP group radio view) The **undo radio disable** command enables specified radios on all APs in an AP group.

(AP radio view) The **radio disable** command disables a specified radio on a single AP.

(AP radio view) The **undo radio disable** command restores the state of a specified radio on an AP to the radio state in the AP group radio view.

By default, radios on all AP are enabled.

Format

radio disable

undo radio disable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to enable or disable a specified radio.

If radio calibration is enabled on an AP, radio calibration is triggered to fill coverage holes after the radio is disabled for 8 minutes.

Example

Disable radio 0 on AP 0 .

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] radio 0
[HUAWEI-wlan-radio-0/0] radio disable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.128 radio-2g-profile (WLAN view)

Function

The **radio-2g-profile** command creates a 2G radio profile and displays the 2G radio profile view, or displays the view of an existing 2G radio profile.

The **undo radio-2g-profile** command deletes a 2G radio profile.

By default, the system provides the 2G radio profile **default**.

Format

radio-2g-profile name *profile-name*

undo radio-2g-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a 2G radio profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all 2G radio profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A 2G radio profile is used to configure and optimize the 2.4 GHz radio of an AP, but does not take effect on the 5 GHz radio.

Follow-up Procedure

Run the **radio-2g-profile** command to apply the 2G radio profile in the AP view, AP group view, AP radio view, or AP group radio view so that the 2G radio profile can take effect.

Precautions

- The 2G radio profile **default** cannot be deleted.
- The 2G radio profile referenced cannot be deleted. To delete the 2G radio profile, unbind it first.

Example

Create the 2G radio profile **radio-profile1** and display the view of the profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio-profile1
[HUAWEI-wlan-radio-2g-prof-radio-profile1]
```


11.1.129 radio-2g-profile

Function

The **radio-2g-profile** command binds a 2G radio profile to a 2G radio.

The **undo radio-2g-profile** command unbinds a 2G radio profile from a 2G radio.

By default, no 2G radio profile is applied in the AP view or AP radio view, but the 2G radio profile **default** is applied in the AP group view and AP group radio view.

Format

radio-2g-profile *profile-name* **radio** { *radio-id* | **all** }

undo radio-2g-profile radio { *radio-id* | **all** }

The parameter **radio** { *radio-id* | **all** } is supported only in the AP group view and AP view.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a 2G radio profile.	The 2G radio profile must exist.
radio *radio-id*	Specifies a radio ID.	The value can be 0 or 2.
radio all	Specifies all radios.	-

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a 2G radio profile using the **radio-2g-profile (WLAN view)** command, bind it to a 2.4 GHz radio so that the 2G radio profile can take effect.

Precautions

After a 2G radio profile is applied in the AP group view or AP view, the parameter settings in the profile take effect on all 2.4 GHz radios on APs in the AP group or on the AP.

The configuration in the AP view and AP radio view has a higher priority than that in the AP group view and AP group radio view.

Example

Create the 2G radio profile **radio-profile1** and bind it to the AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio-profile1
[HUAWEI-wlan-radio-2g-prof-radio-profile1] quit
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio-2g-profile radio-profile1 radio 0
```

11.1.130 radio-5g-profile (WLAN view)

Function

The **radio-5g-profile** command creates a 5G radio profile and displays the 5G radio profile view, or displays the view of an existing 5G radio profile.

The **undo radio-5g-profile** command deletes a 5G radio profile.

By default, the system provides the 5G radio profile **default**.

Format

radio-5g-profile name *profile-name*

undo radio-5g-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a 5G radio profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all 5G radio profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A 5G radio profile is used to configure and optimize the 5 GHz/6 GHz radio of an AP, but does not take effect on the 2.4 GHz radio.

Follow-up Procedure

Run the **radio-5g-profile** command to apply the 5G radio profile in the AP view, AP group view, AP radio view, or AP group radio view so that the 5G radio profile can take effect.

Precautions

- The 5G radio profile **default** cannot be deleted.
- A 5G radio profile referenced cannot be deleted. To delete the 5G radio profile, unbind it first.

Example

Create the 5G radio profile **radio-profile2** and display the view of the profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name radio-profile2
[HUAWEI-wlan-radio-5g-prof-radio-profile2]
```

11.1.131 radio-5g-profile

Function

The **radio-5g-profile** command binds a 5G radio profile to a 5 GHz or 6 GHz radio.

The **undo radio-5g-profile** command unbinds a 5G radio profile from a 5 GHz or 6 GHz radio.

By default, no 5G radio profile is applied in the AP view or AP radio view, but the 5G radio profile **default** is applied in the AP group view and AP group radio view.

Format

radio-5g-profile *profile-name* **radio** { *id* | **all** }

undo radio-5g-profile radio { *id* | **all** }

The parameter **radio** { *id* | **all** } is supported only in the AP group view and AP view.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a 5G radio profile.	The 5G radio profile must exist.
radio *id*	Specifies a radio ID.	The value is an integer that ranges from 0 to 2.
radio all	Specifies all radios.	-

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a 5G radio profile using the **radio-5g-profile (WLAN view)** command, bind it to a 5 GHz radio so that the 5G radio profile can take effect.

Precautions

After a 5G radio profile is applied in the AP group view or AP view, the parameter settings in the profile take effect on all 5 GHz radios on APs in the AP group or on the AP.

The configuration in the AP view and AP radio view has a higher priority than that in the AP group view and AP group radio view.

Example

Create the 5G radio profile **radio-profile2** and bind it to the AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name radio-profile2
[HUAWEI-wlan-radio-2g-prof-radio-profile2] quit
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio-5g-profile radio-profile2 radio 1
```

11.1.132 radio-mode

Function

The **radio-mode** command sets the radio mode of an AP.

The **undo radio-mode** command restores the default radio mode for an AP.

By default, no radio mode is configured on an AP, and the default radio mode of the AP is used.

Format

radio-mode { **2radio-standard** | **2radio-2g-enhanced** | **2radio-5g-enhanced** | **2radio-independent-scan** | **3radio** }

undo radio-mode

Parameters

Parameter	Description	Value
2radio-standard	Specifies the standard dual-radio mode.	-
2radio-2g-enhanced	Specifies the 2G enhanced dual-radio mode. Compared with the standard dual-radio mode, the 2.4 GHz radio in this mode provides more spatial streams and higher throughput. For details, see the specifications of the corresponding AP model.	-
2radio-5g-enhanced	Specifies the 5G enhanced dual-radio mode. Compared with the standard dual-radio mode, the 5 GHz radio in this mode provides more spatial streams and higher throughput. For details, see the specifications of the corresponding AP model.	-
2radio-independent-scan	Specifies the dual-radio + independent scanning radio mode. With the independent scanning radio, functions such as air scan can be implemented without affecting service experience.	-
3radio	Specifies the three-radio mode. A third radio (radio 2) is available to allow access of more STAs.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

The **radio-mode** command sets the radio mode of an AP. Radio modes supported by APs vary depending on AP models. You can check the field **Radio mode** in the **display ap-type id** *ap-type-id* command output for the radio modes supported by a specified AP model. If an AP does not support the configured radio mode, it works in the default radio mode.

- When air interface resources are sufficient, the three-radio mode is recommended to increase the capacity.
- When air interface resources are insufficient, interference is severe, or APs are densely deployed, the dual-radio mode is recommended to reduce interference.

If allowed by the AP capability:

- Dual-radio mode: recommended in large-bandwidth scenarios. In this mode, the AP can provide high throughput.
- Three-radio mode: recommended in high-concurrency scenarios. In this mode, the AP allows for access of more STAs, improving the WLAN capacity.
- Dual-radio + independent scanning radio mode: recommended in high-interference scenarios. In this mode, the AP can use an independent radio to scan air interfaces without affecting performance, thereby achieving real-time monitoring and optimization for WLAN network quality.

NOTE

- Switching the radio mode will cause an AP to restart.
- For an AirEngine 6760-X1 or AirEngine 6760-X1E, load the RTU license to switch to the triple-radio mode or dual-radio + independent scanning mode. For an AirEngine 5760-51, load the RTU license to switch to the dual-radio + independent scanning mode.
- The independent radio scanning function applies only to the 5 GHz radios of the AirEngine 8760-X1-PRO, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, and AirEngine 5760-51. The radio scanning function on the 2.4 GHz frequency band can be implemented only through a service radio. In V200R021C10 and later versions, the independent radio scanning function of the AirEngine 6761-21, AirEngine 6761-21E and AirEngine 6761S-21 is effective for both the 2.4 GHz and 5 GHz frequency bands. (In V200R021C00, this function applies only to the 5 GHz frequency band.)
- The AirEngine 6761-21, AirEngine 6761-21E, and AirEngine 6761S-21 have a dedicated radio for scanning and can perform radio scanning even in **2radio-standard** mode.
- After the radio mode of an AirEngine 6760-51EI is switched to the 2G enhanced dual-radio mode, the 2.4 GHz radio provides four streams and the 5 GHz radio becomes unavailable. After the radio mode is switched to the 5G enhanced dual-radio mode, the 5 GHz radio provides four streams and the 2.4 GHz radio becomes unavailable.

Example

Configure the standard dual-radio mode for the AP.

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



```
[HUAWEI-wlan-view] ap-system-profile name default
[HUAWEI-wlan-ap-system-prof-default] radio-mode 2radio-standard
```

11.1.133 radio-type (2G radio profile view)

Function

The **radio-type** command sets the radio type in a 2G radio profile.

The **undo radio-type** command restores the default radio type in a 2G radio profile.

By default, the radio type in a 2G radio profile is **dot11be**.

Format

radio-type { **dot11b** | **dot11g** | **dot11n** | **dot11ax** | **dot11be** }

undo radio-type

Parameters

Parameter	Description	Value
dot11b	Specifies the 802.11b radio type.	-
dot11g	Specifies the 802.11g radio type, which is backward compatible.	-
dot11n	Specifies the 802.11n radio type, which is backward compatible.	-
dot11ax	Specifies the 802.11ax radio type, which is backward compatible.	-
dot11be	Specifies the 802.11be radio type, which is backward compatible.	-

Views

2G radio profile

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Usually, the default radio type is used and does not need to be modified. If the default radio mode cannot meet requirements or a fault needs to be located, configure the radio type as required.

Precautions

If the configured radio type is not supported by an AP, the actual radio type supported by the AP takes effect.

If a rate in the basic rate set or supported rate set, or the multicast rate is not supported by the 802.11b protocol, the radio type cannot be set to **dot11b**.

If you run the **radio-type dot11b** command in the 2G radio profile view to set the radio type to **dot11b**, and the 2G radio profile is applied to an AP, the rates of management frames and multicast packets that take effect on the 2.4 GHz radio of the AP are fixed as 1 Mbit/s, and the values configured using the **beacon-2g-rate** *beacon-2g-rate* and **multicast-rate** *multicast-rate* commands do not take effect on the AP.

When the L-SIG field length compatibility function of the 802.11n protocol is enabled, the radio type cannot be set to **dot11ax** or **dot11be**.

Example

Set the radio type to **dot11g** in a 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] radio-type dot11g
```

11.1.134 radio-type (5G radio profile view)

Function

The **radio-type** command sets the radio type in a 5G radio profile.

The **undo radio-type** command restores the default radio type in a 5G radio profile.

By default, the radio type in a 5G radio profile is **dot11be**.

Format

radio-type { **dot11a** | **dot11n** | **dot11ac** | **dot11ax** | **dot11be** }

undo radio-type

Parameters

Parameter	Description	Value
dot11a	Specifies the 802.11a radio type.	-
dot11n	Specifies the 802.11n radio type, which is backward compatible.	-
dot11ac	Specifies the 802.11ac radio type, which is backward compatible.	-
dot11ax	Specifies the 802.11ax radio type, which is backward compatible.	-

Parameter	Description	Value
dot11be	Specifies the 802.11be radio type, which is backward compatible.	-

Views

5G radio profile

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Usually, the default radio type is used and does not need to be modified. If the default radio mode cannot meet requirements or a fault needs to be located, configure the radio type as required.

Precautions

If the configured radio type is not supported by an AP, the actual radio type supported by the AP takes effect.

When the L-SIG field length compatibility function of the 802.11n protocol is enabled, the radio type cannot be set to **dot11ax** or **dot11be**.

Example

Set the radio type to **dot11n** in a 5G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] radio-type dot11n
```

11.1.135 reach-max-sta

Function

The **reach-max-sta** command controls access of new STAs when the number of STAs of a VAP reaches the maximum value.

The **undo reach-max-sta** command cancels the configuration.

By default, when the number of access users reaches the maximum value, you can determine whether to enable SSID hiding or enable the VAP to replace low-priority STAs with high-priority STAs.

Format

reach-max-sta { **hide-ssid disable** | **priority-replace** }

undo reach-max-sta

Parameters

Parameter	Description	Value
hide-ssid disable	Disable SSID hiding.	-
priority-replace	Enable the VAP to replace low-priority STAs with high-priority STAs.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

When the number of access users reaches the maximum value, you can enable SSID hiding or enable the VAP to replace low-priority STAs with high-priority STAs. The two functions cannot be configured simultaneously.

- SSID hiding: New STAs cannot search for the SSID of the VAP and need to access other VAPs.
- Replacing low-priority STAs with high-priority STAs: A new VIP user will replace a common user. This ensures access experience of VIP users.

Example

Disable automatic SSID hiding when the number of users reaches the maximum.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] reach-max-sta hide-ssid disable
```

11.1.136 regulatory-domain-profile (WLAN view)

Function

The **regulatory-domain-profile** command creates a regulatory domain profile and displays the regulatory domain profile view, or displays the view of an existing regulatory domain profile.

The **undo regulatory-domain-profile** command deletes a regulatory domain profile.

By default, the system provides the regulatory domain profile **default**.

Format

regulatory-domain-profile name *profile-name*

undo regulatory-domain-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a regulatory domain profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all regulatory domain profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A regulatory domain profile contains settings of the country code, calibration channel, and calibration bandwidth, which take effect on APs using the regulatory domain profile.

Follow-up Procedure

Run the **regulatory-domain-profile** command to bind the regulatory domain profile to an AP or AP group so that the regulatory domain profile can take effect.

Precautions

- The regulatory domain profile **default** cannot be deleted.
- The regulatory domain profile referenced by an AP or AP group cannot be deleted. To delete the regulatory domain profile, unbind it from the AP or AP group first.

Example

Create the regulatory domain profile **domain1** and display the regulatory domain profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name domain1
[HUAWEI-wlan-regulate-domain-domain1]
```

11.1.137 regulatory-domain-profile

Function

The **regulatory-domain-profile** command binds a regulatory domain profile to an AP or AP group.

The **undo regulatory-domain-profile** command unbinds a regulatory domain profile from an AP or AP group.

By default, the regulatory domain profile **default** is bound to an AP group, but no regulatory domain profile is bound to an AP. In the default regulatory domain profile, the country code is China, 2.4G calibration channels include channels 1, 6, and 11, 5G calibration channels include channels 149, 153, 157, 161, and 165, the 5G calibration bandwidth is 20 MHz, and the wideband function is disabled.

Format

regulatory-domain-profile *profile-name*

undo regulatory-domain-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a regulatory domain profile.	The regulatory domain profile must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a regulatory domain profile using the **regulatory-domain-profile (WLAN view)** command, bind it to an AP or AP group so that the regulatory domain profile can take effect.

Precautions

After a regulatory domain profile is bound to an AP or AP group, parameter settings in the regulatory domain profile apply to all APs using the profile.

Example

Create the regulatory domain profile **domain1** and bind it to AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name domain1
[HUAWEI-wlan-regulate-domain-domain1] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may restart APs. Continue?[Y/N]:y
```

11.1.138 report-disassoc-request disable

Function

The **report-disassoc-request disable** command disables an AP from reporting disassociation request packets of STAs to the AC.

The **undo report-disassoc-request disable** command enables an AP to report disassociation request packets of STAs to the AC.

By default, an AP is enabled to report disassociation request packets of STAs to the AC.

Format

report-disassoc-request disable

undo report-disassoc-request disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If a large number of STAs disassociate from the network in a certain time, the APs need to report lots of disassociation request packets to the AC, impacting the AC

performance. To alleviate the impact on the AC, you can disable APs from reporting disassociation request packets of STAs to the AC.

Example

Disable an AP from reporting disassociation request packets of STAs to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ab
[HUAWEI-wlan-ap-system-prof-ab] report-disassoc-request disable
```

11.1.139 report-sta-assoc enable

Function

The **report-sta-assoc enable** command enables the function of recording STA association information or STA login information in the log.

The **undo report-sta-assoc enable** command disables the function of recording STA association information or STA login information in the log.

By default, the function of recording STA association information or STA login information in the log is disabled.

Format

report-sta-assoc enable

undo report-sta-assoc enable

Parameters

None

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

If a STA is associated or goes online after this function is enabled, the device records the STA association or login information in the log.

NOTE

Enabling this function will generate a large number of logs. If there are a large number of STAs, log files may overwrite each other due to limited storage space, which affects fault locating. To enable this function, you are advised to configure a log server to report logs. For details, choose **Configuring Information Center** > **Configuring Log Output** in the *Configuration Guide*.

Example

Enable the function of recording STA association information or STA login information in the log.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] report-sta-assoc enable
Warning: This operation will generate a large number of logs, which may overwrite other logs.
Configuring a log server is recommended. Continue?[Y/N]:y
```

11.1.140 report-sta-info enable

Function

The **report-sta-info enable** command enables an AC to report information about STA traffic statistics and online duration on APs.

The **undo report-sta-info enable** command disables an AC from reporting information about STA traffic statistics and online duration on APs.

By default, an AC is disabled from reporting information about STA traffic statistics and online duration on APs.

Format

report-sta-info enable

undo report-sta-info enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **report-sta-info enable** command to enable an AC to report information about STA traffic statistics and online duration on APs to eSight. After this function is enabled, the AC collects and reports information about STA traffic statistics and online duration on APs to eSight through syslogs when STAs get offline or roam within the AC, which facilitates data query on eSight. The STA traffic statistics include the AC's MAC address, AC name, APs' MAC addresses, AP names, radio IDs, SSID, user names, and STAs' MAC addresses.

NOTE

Enabling this function will generate a large number of logs. If there are a large number of STAs, log files may overwrite each other due to limited storage space, which affects fault locating. To enable this function, you are advised to configure a log server to report logs. For details, choose **Configuring Information Center** > **Configuring Log Output** in the *Configuration Guide*.

Example

Enable an AC to report information about STA traffic statistics and online duration on APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] report-sta-info enable
Warning: This operation will generate a large number of logs, which may overwrite other logs.
Configuring a log server is recommended. Continue?[Y/N]:y
```

11.1.141 reset ap offline-record

Function

The **reset ap offline-record** command clears AP going-offline records.

Format

reset ap offline-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Clears going-offline records of all APs.	-
mac *mac-address*	Clears going-offline records of the AP with specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-collect AP going-offline records, run this command to clear existing records.

Precautions

The cleared records cannot be restored.

Example

Clear going-offline records of all APs.

```
<HUAWEI> reset ap offline-record all
```

11.1.142 reset ap online-fail-record

Function

The **reset ap online-fail-record** command clears AP online failure records.

Format

reset ap online-fail-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Clears online failure records of all APs.	-
mac *mac-address*	Clears online failure records of the AP with the specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-collect records about AP online failures, run this command to clear existing records first.

Precautions

The cleared records cannot be restored.

Example

Clear online failure records of all APs.

```
<HUAWEI> reset ap online-fail-record all
```


11.1.143 reset ap unauthorized record

Function

The **reset ap unauthorized record** command clears information about unauthorized APs.

Format

reset ap unauthorized record

Parameters

None

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to clear the unauthorized AP list so that removed APs or unauthenticated APs that are physically disconnected from the AC can be cleared. This helps users easily collect statistics and confirm unauthorized APs.

Precautions

If an AP physically connects to the AC but has not been authenticated, the AP is added to the unauthorized AP list after you run the **reset ap unauthorized record** command.

Example

Clear information about unauthorized APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] reset ap unauthorized record
Warning: Clear unauthorized AP record, continue?[Y/N]:y
```

11.1.144 reset channel switch-record

Function

The **reset channel switch-record** command deletes channel switching records on a device.

Format

reset channel switch-record all

Parameters

Parameter	Description	Value
all	Deletes all channel switching records.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to delete existing channel switching records so that the system can record new channel switching events.

Precautions

Deleted channel switching records cannot be restored.

Example

Delete all channel switching records.

```
<HUAWEI> reset channel switch-record all
```

11.1.145 reset station assoc-info ap-offline-record

Function

The **reset station assoc-info ap-offline-record** command deletes information about STAs that connect to the APs in fault state.

Format

reset station assoc-info ap-offline-record { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Deletes information about all STAs that connect to APs in fault state from the AC.	-
ap-name *ap-name*	Clears information about STAs that go online on the AP with a specified name in fault state.	The AP name must exist.
ap-id *ap-id*	Clears information about STAs that go online on the AP with a specified ID in fault state.	The AP ID must exist.
radio *radio-id*	Deletes information about STAs that connect to the specified radio of the AP in fault state.	The radio ID must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics on the STAs that connect to the APs in fault state within a specific period, run the **reset station assoc-info ap-offline-record** command to delete the original STA information.

Prerequisites

The APs in fault state have been enabled to allow access of new STAs using the **keep-service enable allow new-access** command.

Function

The deleted STA information cannot be restored. Exercise caution when you run the **reset station assoc-info ap-offline-record** command.

Example

Delete information about all STAs that connect to APs in fault state from the AC.

```
<HUAWEI> reset station assoc-info ap-offline-record all
```


11.1.146 reset station offline-record

Function

The **reset station offline-record** command deletes STAs' going-offline records.

Format

reset station offline-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac* }

Parameters

Parameter	Description	Value
all	Deletes going-offline records of all STAs.	-
ap-name *ap-name*	Deletes STAs' going-offline records on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Deletes STAs' going-offline records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac*	Deletes going-offline records of a specified STA.	The STA's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to delete existing STAs' going-offline records so that the system can record new STAs' going-offline events.

Precautions

The deleted records cannot be restored.

Example

Delete going-offline records of all STAs.

```
<HUAWEI> reset station offline-record all
```


11.1.147 reset station online-fail-record

Function

The **reset station online-fail-record** command deletes records of STAs' failures to go online.

Format

reset station online-fail-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac-address* }

Parameters

Parameter	Description	Value
all	Deletes records of all STAs' failures to go online.	-
ap-name *ap-name*	Deletes records of STAs' failures to go online on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Deletes records of STAs' failures to go online on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac-address*	Deletes records of failures to go online of the STA with a specified MAC address.	The STA's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to delete existing records of STAs' failures to go online so that the system can record new failures of STAs to go online.

Precautions

The deleted records cannot be restored.

Example

Delete records of all STAs' failures to go online.

```
<HUAWEI> reset station online-fail-record all
```


11.1.148 reset station statistics

Function

The **reset station statistics** command deletes statistics about online STAs.

Format

reset station statistics [**sta-mac** *sta-mac-address*]

Parameters

Parameter	Description	Value
sta-mac *sta-mac-address*	Specifies the MAC address of an online STA.	The STA's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting statistics about online STAs, run the command to clear the existing statistics.

Precautions

After the command is run, statistics about online STAs are cleared and cannot be restored.

Example

Delete statistics about the STA with MAC address 00e0-fc88-b74f.

```
<HUAWEI> reset station statistics sta-mac 00e0-fc88-b74f
```

11.1.149 rf-ping

Function

The **rf-ping** command enables an AP to proactively detect wireless link quality.

NOTE

The rf-ping function is not supported on the following APs.

- AirEngine x762

Format

rf-ping [**-m** *time* | **-c** *number* | **-p** { **be** | **bk** | **vi** | **vo** }] * *mac-address*

Parameters

Parameter	Description	Value
-m *time*	Specifies the interval for sending probe data packets.	The value is an integer that ranges from 100 to 10000, in milliseconds. The default value is 100.
-c *number*	Specifies the number of probe data packets sent by the AP.	The value is an integer that ranges from 1 to 1000. The default value is 10.
-p { **be** | **bk** | **vi** | **vo** }	Specifies the priority of probe data packets sent by the AP, which can be AC_BE, AC_BK, AC_VI, or AC_VO. If this parameter is not specified, the default priority is AC_BE.	-
mac-address	Specifies the MAC address of a STA.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can be used to obtain parameters of wireless links between APs and STAs, including the signal strength, air interface rate, and packet transmission delay.

Prerequisites

STAs have been associated with the APs and gone online.

Example

Configure an AP to automatically detect the quality of the wireless link with the STA whose MAC address is 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rf-ping 00e0-fc12-3456
 Tx rate=52.0 Mbps, Reply from 00e0-fc12-3456: RSSI=-58 dBm time < 1 ms
 1 packets transmitted, 1 received, 0% packet loss, time < 1 ms, RSSI -58 dBm
```

Table 11-65 Description of the **rf-ping** command output

Item	Description
Tx rate	Transmit rate.
Reply from	STA's MAC address.
RSSI	Received signal strength.
time	Delay.
x packets transmitted	*x* packets are transmitted.
x received	*x* packets are received.
x% packet loss	Packet loss rate.

11.1.150 rts-cts-mode

Function

The **rts-cts-mode** command sets the request to send (RTS)-clear to send (CTS) operation mode in a radio profile.

The **undo rts-cts-mode** command restores the default RTS-CTS operation mode in a radio profile.

By default, the RTS-CTS operation mode is **rts-cts**.

Format

rts-cts-mode { **cts-to-self** | **disable** | **rts-cts** }

undo rts-cts-mode

Parameters

Parameter	Description	Value
cts-to-self	Sets the RTS-CTS operation mode to **cts-to-self** (only supported in the 2G radio profile view).	-
disable	Disables RTS-CTS.	-
rts-cts	Sets the RTS-CTS operation mode to **rts-cts**.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

- In **rts-cts** mode, an AP sends an RTS frame before sending data to a STA. After receiving the RTS frame, all the devices within the coverage of the AP do not send data within the specified time. Upon receiving the RTS frame, the target STA sends a CTS frame. This ensures that all the devices within the coverage of the STA do not send data within the specified time. This mode avoids conflicts but involves transmission of two frames (RTS and CTS frames), increasing the overhead.
- In **cts-to-self** mode, an AP sends a CTS frame with the AP's own address as the receiver address (RA) before sending data to a STA. This ensures that all the devices within the coverage of the AP do not send data within the specified time. In most scenarios, this mode allows an AP to only send one frame to avoid channel conflicts. However, if there is a device within the STA's coverage area but not within the AP's coverage area, a channel conflict may still occur.

Compared to the **rts-cts** mode, the **cts-to-self** mode reduces the number of control frames transmitted on the network. In some cases, however, a channel conflict may still occur when a hidden node exists and does not receive the CTS frame from the AP. Therefore, the **rts-cts** mode is more effective in avoiding channel conflicts than the **cts-to-self** mode.

To avoid the data transmission failure caused by a channel conflict, run this command to set the RTS-CTS operation mode in a radio profile as required.

Example

Set the RTS-CTS operation mode to **rts-cts** in a 2G radio profile.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] rts-cts-mode rts-cts
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.151 rts-cts-threshold

Function

The **rts-cts-threshold** command sets the RTS-CTS threshold in a radio profile.

The **undo rts-cts-threshold** command restores the default RTS-CTS threshold in a radio profile.

The default RTS-CTS alarm threshold is 1400 bytes.

Format

rts-cts-threshold *rts-cts-threshold*

undo rts-cts-threshold

Parameters

Parameter	Description	Value
rts-cts-threshold	Specifies the RTS-CTS threshold. If the length of a frame to be sent by the MAC Layer exceeds this threshold, an RTS frame needs to be sent before this frame.	The value is an integer that ranges from 64 to 2347, in bytes.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

The IEEE 802.11 MAC protocol provides an RTS-CTS handshake protocol to prevent conflicts between channels and failure to transmit data. STA A sends an RTS frame before sending data to STA B. STA A can send data after receiving a CTS frame from STA B. If multiple STAs send RTS frames to the same STA, only the STA that receives a CTS frame can send data, and other STAs must wait for a certain period and then send RTS frames again.

If STAs implement RTS-CTS handshakes before sending data, the channel bandwidth is consumed by too much RTS frames. You can set an RTS threshold to specify the length of frames to be sent. When the length of frames to be sent by the STA is smaller than the RTS threshold, no RTS/CTS handshake is implemented.

Example

Set the RTS-CTS threshold to 2300 bytes in the 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] rts-cts-threshold 2300
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.152 rx-stbc disable

Function

The **rx-stbc disable** command disables the space-time block coding (STBC) function in the receive direction.

The **undo rx-stbc disable** command enables the STBC function in the receive direction.

By default, the STBC function in the receive direction is enabled.

NOTE

The STBC function in the receive function is unconfigurable and always enabled for the following models:

- AirEngine x761
- AirEngine x762
- AirEngine x771

Format

rx-stbc disable

undo rx-stbc disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

STBC is a coding technology used in Wi-Fi standards. It uses time and space diversity in a multi-antenna system to transmit the same data over multiple antennas to improve data transmission reliability.

If severe packet loss occurs on a STA that uses STBC to send packets, it is recommended that the STBC function be disabled in the receive direction of the AP.

Example

Disable the STBC function in the receive direction in the 2G radio profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] rx-stbc disable
```

11.1.153 service-mode disable

Function

The **service-mode disable** command disables the service mode of a VAP.

The **undo service-mode disable** command enables the service mode of a VAP.

By default, the service mode of a VAP is enabled.

Format

service-mode disable

undo service-mode disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **service-mode disable** command to disable the service mode of a VAP. After the service mode of a VAP is disabled, the VAP is disabled.

- After the service mode of a VAP is enabled, run the **auto-off service** command to enable the scheduled VAP auto-off function. In the scheduled time, the VAP is disabled. To enable the VAP, run the **undo auto-off service** command.
- After the service mode of a VAP is disabled, the scheduled VAP auto-off function does not take effect.

Example

Disable the service mode of VAP **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] service-mode disable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.154 service-vlan (VAP profile view)

Function

The **service-vlan** command configures a service VLAN for a VAP.

The **undo service-vlan** command restores the default service VLAN of a VAP.

By default, VLAN 1 is the service VLAN of a VAP.

Format

service-vlan { **vlan-id** *vlan-id* | **vlan-pool** *pool-name* }

undo service-vlan

Parameters

Parameter	Description	Value
vlan-id *vlan-id*	Specifies a service VLAN ID of a VAP.	The value is an integer that ranges from 1 to 4094.
vlan-pool *pool-name*	Sets the service VLANs of a VAP to all VLANs in a VLAN pool.	The VLAN pool must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can specify a specific VLAN as the service VLAN of a VAP or all VLANs in a VLAN pool as the service VLANs of a VAP. Layer 2 data packets delivered from the VAP to an AP carry the service VLAN IDs.

- When a specific VLAN is configured as the service VLAN of a VAP, STAs connected to the VAP join the same VLAN.

- When VLANs in a VLAN pool are configured as the service VLANs of a VAP, STAs connected to the VAP join different VLANs. The VLAN assignment algorithm can be configured using the **assignment** command.

Precautions

Modifying the service VLAN of a VAP will interrupt services of STAs connected to the VAP. Exercise caution when you run the command.

Example

Set the service VLAN to VLAN 2 in the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] service-vlan vlan-id 2
```

11.1.155 short-preamble disable

Function

The **short-preamble disable** command configures a radio profile not to support the short preamble.

The **undo short-preamble disable** command configures a radio profile to support the short preamble.

By default, a radio profile supports the short preamble.

Format

short-preamble disable

undo short-preamble disable

Parameters

None

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

The preamble is a section of bits in the header of a data frame. It synchronizes signals transmitted between the sender and receiver. The preamble is classified into the long preamble and short preamble. The short preamble ensures better synchronization performance and therefore is recommended. The long preamble is usually used for compatibility with earlier network adapters of clients.

Example

Configure the 2G radio profile **default** not to support the short preamble.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] short-preamble disable
```

11.1.156 single-txchain enable

Function

The **single-txchain enable** command enables the single-antenna transmission mode.

The **undo single-txchain enable** command disables the single-antenna transmission mode.

By default, the single-antenna transmission mode is disabled.

Format

single-txchain enable

undo single-txchain enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some non-HT STAs that support 802.11a/b/g cannot receive packets sent by APs using multiple antennas. As a result, network access failures, frequent STA roaming, or network instability is caused. After running the **single-txchain enable** command to enable the single-antenna transmission mode in an SSID profile, management packets on the corresponding VAP and data packets sent by the AP to non-HT STAs on the VAP will be sent in single-antenna transmission mode. For a radio that is bound to a VAP with the single-antenna transmission mode enabled, control packets of the radio are sent in single-antenna transmission mode as long as non-HT STAs is connected to the VAP. When no non-HT STA is connected to the VAP, the control packets are still sent in multi-antenna transmission mode.

Precautions

APs supporting MU-MIMO support the single-antenna transmission mode.

After the single-antenna transmission mode is enabled in an SSID profile, the RSSI of STAs may be affected.

Example

Enable the single-antenna transmission mode in SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] single-txchain enable
```

11.1.157 softgre-profile (WLAN view)

Function

The **softgre-profile** command creates a soft GRE profile and displays its view, or displays the view of an existing soft GRE profile.

The **undo softgre-profile** command deletes a soft GRE profile.

By default, no soft GRE profile exists in the system.

Format

softgre-profile name *profile-name*

undo softgre-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a soft GRE profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all soft GRE profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the data forwarding mode is set to **soft-GRE**, create a soft GRE profile and bind it to a VAP profile for the soft GRE profile to take effect.

To configure parameters in a soft GRE profile, run this command to enter the soft GRE profile view. If a soft GRE profile is no longer needed, you can delete it.

Follow-up Procedure

Run the **forward-mode** command to bind the soft GRE profile to a VAP profile so that the soft GRE profile can take effect.

Precautions

The soft GRE profile referenced by a VAP profile cannot be deleted. To delete the soft GRE profile, unbind it from the VAP profile first.

Example

Create the soft GRE profile **soft1** and enter the soft GRE profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] softgre-profile name soft1
[HUAWEI-wlan-softgre-prof-soft1]
```

11.1.158 ssid

Function

The **ssid** command sets a service set identifier (SSID) for an SSID profile.

The **undo ssid** command deletes the SSID of an SSID profile.

By default, the SSID HUAWEI-WLAN is configured in an SSID profile.

Format

ssid *ssid*

undo ssid

Parameters

Parameter	Description	Value
ssid	Specifies the name of an SSID.	The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters. To start an SSID with a space, you need to encompass the SSID with double quotation marks (" "), for example, **" hello"**. The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to add a backslash (\) before the double quotation mark, for example, **\"hello**. The backslash occupies one character. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters. SSIDs containing Chinese characters cannot be displayed on STAs that do not support the UTF-8 encoding format.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSID specifies a wireless network. When you search for available wireless networks on your wireless terminal, SSIDs are displayed to identify the available wireless networks.

Precautions

When you configure an SSID containing Chinese characters, do not delete characters by pressing the **Delete** button if you want to modify the SSID that has been entered. Otherwise, the SSID will contain garbled characters after the configuration. In this case, run the **ssid** command to reconfigure the SSID.

Example

Set the SSID to **wlan-net** in the SSID profile **ssid1**.

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



```
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] ssid wlan-net
```

11.1.159 ssid-hide enable

Function

The **ssid-hide enable** command enables SSID hiding in Beacon frames in an SSID profile.

The **undo ssid-hide enable** command disables SSID hiding in Beacon frames in an SSID profile.

By default, SSID hiding in Beacon frames is disabled in an SSID profile.

Format

ssid-hide enable

undo ssid-hide enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A STA listens on the Beacon frames that an AP periodically sends in each channel to obtain AP information. The STA can obtain SSIDs from Beacon frames that contain the SSIDs.

The STA can actively send a probe frame with a specified SSID, only the AP with the same SSID will respond to the STA. If the STA broadcasts a probe frame without an SSID, only the APs on which SSID hiding in Beacon frames is disabled will respond to the STA.

- After the **ssid-hide enable** command is used, an AP periodically sends Beacon frames that contain empty SSID character strings and does not reply to the broadcast probe requests sent from STAs. The STAs can send probe frames with the AP's SSID to discover the SSID.
- After the **undo ssid-hide enable** command is used, an AP periodically sends Beacon frames that contain valid SSID character strings and replies to the broadcast probe requests sent from STAs. The STAs can send probe frames with the AP's SSID to discover the SSID.

Precautions

If the **ssid-hide enable** or **undo ssid-hide enable** command is run in the SSID profile after STAs are associated with an SSID, service interruptions may occur for all online STAs.

Example

Configure SSID hiding in Beacon frames in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] ssid-hide enable
```

11.1.160 ssid-profile (WLAN view)

Function

The **ssid-profile** command creates an SSID profile and displays the SSID profile view, or displays the view of an existing SSID profile.

The **undo ssid-profile** command deletes an SSID profile.

By default, the system provides the SSID profile **default**.

Format

ssid-profile name *profile-name*

undo ssid-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an SSID profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all SSID profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSID profile is used to configure STA association and access parameters based on SSIDs, including the SSID name, STA association timeout period, non-HT STA access, and QoS CAR.

Follow-up Procedure

Run the **ssid-profile (VAP profile view)** command in the VAP profile view to bind the SSID profile to the VAP profile, and then bind the VAP profile to an AP, so that the SSID profile can take effect.

Precautions

- The SSID profile **default** cannot be deleted.
- An SSID profile referenced by a VAP profile cannot be deleted. To delete the SSID profile, unbind it from the VAP profile first.
- If a VAP profile has been applied to an AP, modifying the SSID profile will interrupt services.

Example

Create an SSID profile named **ssid1** and enter the SSID profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1]
```

11.1.161 ssid-profile (VAP profile view)

Function

The **ssid-profile** command binds an SSID profile to a VAP profile.

The **undo ssid-profile** command unbinds an SSID profile from a VAP profile.

By default, the SSID profile **default** is bound to a VAP profile.

Format

ssid-profile *profile-name*

undo ssid-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an SSID profile.	The SSID profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an SSID profile using the **ssid-profile (WLAN view)** command, bind it to a VAP profile to make the SSID profile take effect.

Precautions

After an SSID profile is bound to a VAP profile, parameter settings in the SSID profile take effect on all APs using the VAP profile.

Example

Create the SSID profile **ssid1** and bind it to the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] quit
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] ssid-profile ssid1
```

11.1.162 sta-ipv6-service enable

Function

The **sta-ipv6-service enable** command enables the function of processing STA IPv6 services.

The **undo sta-ipv6-service enable** command disables the function of processing STA IPv6 services.

By default, the function of processing STA IPv6 services is disabled.

Format

sta-ipv6-service enable

undo sta-ipv6-service enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Currently, IPv4 WLANs are widely deployed. If many IPv6 packets exist on an IPv4 WLAN, the performance of the WLAN is affected, and the CPU processing capability of devices will also be degraded. To improve performance of a pure IPv4 network, you can configure devices on the network to not process IPv6 packets of STAs.

Precautions

The function of processing STA IPv6 services takes effect only when the following conditions are met:

- In tunnel forwarding mode, the device does not function as an IPv6 gateway. This condition is not required in direct forwarding mode.
- The security policy is open authentication.

After the function of processing STA IPv6 services is disabled:

- The AC and APs do not process IPv6 packets of the wireless side.
- IPv6 functions cannot be configured on the wireless side.
- IPv6 functions of the wireless side are disabled even if they are enabled in default settings.

Running the **ipv6 enable** command in the interface view only enables the IPv6 function on the wired-side interface. The command cannot enable the WLAN module to process STA IPv6 services. To enable the WLAN module to process IPv6 services of STAs, you need to run the **sta-ipv6-service enable** command in the WLAN view.

Example

Enable the function of processing STA IPv6 services.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-ipv6-service enable
```


11.1.163 sta-network-detect disable

Function

The **sta-network-detect disable** command disables network detection upon STA reassociation.

The **undo sta-network-detect disable** command enables network detection upon STA reassociation.

By default, network detection upon STA reassociation is enabled.

Format

sta-network-detect disable

undo sta-network-detect disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

When accessing a new Wi-Fi network, some STAs initiate reassociation requests but not association requests. For example, this may happen when a STA attempts to access a new Wi-Fi network with the same name as the network that the STA has accessed. In this case, the STA considers that the access to the new Wi-Fi network is normal, while it actually fails to access the network. As a result, the STA cannot access network resources. To enable STAs to access the network through the normal process, you can enable network detection upon STA reassociation. When a STA reassociates with the network, the AP forcibly disconnects the STA and enables it to reinitiate an association request to access the network if all of the following conditions are met:

- The STA does not send DHCP Request messages or receive ARP Reply packets within 5s after it reassociates with the AP and goes online.
- The STA has only uplink traffic but no downlink traffic.

Example

Enable network detection upon STA reassociation.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] undo sta-network-detect disable
```


11.1.164 sta-network-detect assoc enable

Function

The **sta-network-detect assoc enable** command enables network detection upon STA association.

The **undo sta-network-detect assoc enable** command disables network detection upon STA association.

By default, network detection upon STA association is disabled.

Format

sta-network-detect assoc enable

undo sta-network-detect assoc enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Some STAs may fail to access the Internet after sending association requests. To enable STAs to access the network through the normal process, you can enable network detection upon STA association. When a STA associates with the network, the AP forcibly disconnects the STA and enables it to reinitiate an association request to access the network if both of the following conditions are met:

- The STA does not send DHCP Request messages or receive ARP Reply packets within 5s after it associates with the AP and goes online.
- The STA has only uplink traffic but no downlink traffic.

Example

Enable network detection upon STA association.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] sta-network-detect assoc enable
```


11.1.165 sta-offline-delay aging-time

Function

The **sta-offline-delay aging-time** command configures the aging time for STA offline delay.

The **undo sta-offline-delay aging-time** command restores the default aging time for STA offline delay.

The default aging time for STA offline delay is 180 seconds.

Format

sta-offline-delay aging-time *time*

undo sta-offline-delay aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time for STA offline delay.	The value is an integer that ranges from 1 to 604800, in seconds. The default value is 180.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STA offline delay function is enabled, STAs can go offline and online again in the aging time without being authenticated, reducing the load on the authentication server. You can run the **sta-offline-delay aging-time** command to set the aging time.

Set the aging time for STA offline delay based on the network requirements and device performance. A long aging time causes the STA offline delay function to occupy many resources, affecting new STA access. A short aging time cannot achieve a noticeable effect in releasing the load on the authentication server.

If 802.1X authentication is used for STAs, it is recommended that set the aging time of the STA offline delay state a value ranging from 1s to 1800s. Within this

range, you can set a longer delay to improve the roaming success rate of fast roaming using PMK caching and 802.11r fast roaming.

Prerequisites

The STA offline delay function has been enabled using the **sta-offline-delay enable** command.

Example

Set the aging time for STA offline delay to 300s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-offline-delay enable
[HUAWEI-wlan-view] sta-offline-delay aging-time 300
```

11.1.166 sta-offline-delay enable

Function

The **sta-offline-delay enable** command enables the STA offline delay function.

The **undo sta-offline-delay enable** command disables the STA offline delay function.

By default, the STA offline delay function is disabled.

Format

sta-offline-delay enable

undo sta-offline-delay enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a WLAN, some online STAs may go offline due to reasons such as screen lock. When these STAs go online again, they are reauthenticated, increasing the load on the authentication server. After the STA offline delay function is enabled, if a STA goes offline normally (for example, by sending a disassociation or deauthentication request or reaching the association aging time) and online again within the aging time, it does not need to be authenticated by an external or

built-in authentication server. This reduces the load on the authentication server and avoids multiple authentication operations. This function takes effect for STAs only in Portal, MAC address, 802.1X, or MAC address-prioritized Portal authentication mode.

NOTE

After the STA offline delay function is enabled, if a STA goes offline normally and online again within the aging time, no authentication is needed. This may bring security risks. Exercise caution when configuring this function.

Precautions

The STA offline delay function is implemented for new access and Layer 2 roaming STAs. When a STA reassociates with a WLAN within the aging time, the STA offline delay function is implemented only in the following scenarios:

- Non-roaming scenarios. That is, the STA goes online again on the same VAP.
- Intra-AC Layer 2 roaming in direct forwarding mode, intra-AC Layer 3 roaming in direct forwarding mode (with the tunnel endpoint on the AC), or intra-AC Layer 2/3 roaming in tunnel forwarding mode.
- Inter-AC Layer 2 roaming in direct or tunnel forwarding mode.

The STA offline delay function and online STA detection on the external Portal server are mutually exclusive.

Example

Enable the STA offline delay function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-offline-delay enable
```

11.1.167 sta-offline-delay full-sta-reject enable

Function

The **sta-offline-delay full-sta-reject enable** command disables an AP to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

The **undo sta-offline-delay full-sta-reject enable** command enables an AP to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

By default, an AP is enabled to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

Format

sta-offline-delay full-sta-reject enable

undo sta-offline-delay full-sta-reject enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STA offline delay function is enabled on an AP, you can run this command to enable an AP to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

Prerequisites

Before this command is executed, the **sta-offline-delay enable** command has been executed to enable the STA offline delay function.

Example

Disable an AP to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-offline-delay enable
[HUAWEI-wlan-view] sta-offline-delay full-sta-reject enable
```

11.1.168 sta-offline-delay max-number

Function

The **sta-offline-delay max-number** command sets the maximum number of STAs that are allowed to delay going offline.

The **undo sta-offline-delay max-number** command restores the default maximum number of STAs that are allowed to delay going offline.

The default maximum number of STAs that are allowed to delay going offline is one fifth of the maximum number of STAs supported by an AC.

Format

sta-offline-delay max-number *max-number*

undo sta-offline-delay max-number

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of STAs that are allowed to delay going offline.	The value is an integer that ranges from 1 to the maximum number of STAs supported by an AC. The default value is one fifth of the maximum value. If one fifth of the maximum value is a non-integer value, round down the value.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STA offline delay function is enabled, you can run this command to set the maximum number of STAs that are allowed to delay going offline.

Set the maximum number of STAs that are allowed to delay going offline based on the network requirements and device performance. A large value causes the STA offline delay function to occupy many resources, affecting new STA access. A small value cannot achieve a noticeable effect in releasing the load on the authentication server.

Prerequisites

The STA offline delay function has been enabled using the **sta-offline-delay enable** command.

Example

Set the maximum number of STAs that are allowed to delay going offline to 800.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-offline-delay enable
[HUAWEI-wlan-view] sta-offline-delay max-number 800
```


11.1.169 station connectivity-detect disable

Function

The **station connectivity-detect disable** command disables STA connectivity check on the AP.

The **undo station connectivity-detect disable** command enables STA connectivity check on the AP.

By default, STA connectivity check is enabled on the AP.

Format

station connectivity-detect disable

undo station connectivity-detect disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

The STA connectivity check function is enabled on an AP by default to help locate the Internet access failure issue of some STAs in certain scenarios. The AP periodically checks the uplink and downlink unicast traffic of STAs. If an exception is detected, the AP randomly selects a certain number of STAs, pings the gateway and STAs to check network connectivity, and logs the check result. After a STA is detected, the STA will not be detected repeatedly within a certain period of time.

Example

Disable STA connectivity check.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name default
[HUAWEI-wlan-ap-system-prof-default] station connectivity-detect disable
```

11.1.170 twt enable

Function

The **twt enable** command enables the target wake time (TWT) function.

The **undo twt enable** command disables the TWT function.

By default, the TWT function is disabled.

Format

twt enable

undo twt enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

TWT is a scheduling algorithm introduced in 802.11ax. A TWT Requesting STA negotiates with a TWT Responding STA (AP) to determine TWT parameters and wake ups for some time called service period (SP). In this manner, STAs can doze always except during the SP intervals, which saves power consumption of the STA and allows an AP to manage activities in the BSS in order to minimize contention between STAs.

It is recommended that the TWT function be disabled if the STA and AP are incompatible with each other due to different protocol implementation modes.

Example

Enable the TWT function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] twt enable
```

11.1.171 type (VAP profile view)

Function

The **type** command sets the type for a VAP.

The **undo type** command restores the default VAP type.

By default, the type of a VAP is service.

Format

type { **ap-management** | **service** | **service-backup ap-offline** | **service-backup auth-server-down radius-server template** *template-name* | **service-backup distribute** }

undo type

Parameters

Parameter	Description	Value
ap-management	Sets the VAP type to AP management.	-
service	Sets the VAP type to service.	-
service-backup ap-offline	Sets the VAP type to AP-offline backup service.	-
service-backup auth-server-down	Sets the VAP type to authentication-server-down backup service.	-
radius-server template *template-name*	Specifies the name of a RADIUS server template.	The specified name of the RADIUS server template must exist.
service-backup distribute	Sets the VAP type to distributed-AP backup service. **NOTE** This parameter takes effect only for the backup AP in the zero-roaming distributed architecture.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- If the type of a VAP is set to **ap-management**, STAs connected to the VAP can only access APs but not network resources. AP management VAPs are used in STA access and AP management scenarios.
- If the type of a VAP is set to **service**, STAs connected to the VAP can only access network resources but not APs. Service VAPs are used in regular WLAN deployment scenarios.
- If the type of a VAP is set to **service-backup ap-offline**, STAs can access the network through the backup service VAP after the AP goes offline. For example, on a headquarters-branch network, when APs at branches connect to the AC at the headquarters through a WAN, APs may go offline due to the WAN instability. In this case, you can configure a backup service VAP to allow new STAs to access the network if the AP goes offline.

- If the type of a VAP is set to **service-backup auth-server-down**, the VAP is automatically enabled to allow network access of associated STAs when the authentication server is not accessible. When the authentication server recovers, this VAP is not automatically disabled. You can manually disable it if needed. If the authentication server is accessible but rejects user access, this VAP is not automatically enabled. You can manually enable it if needed. To enable or disable this VAP, run the **vap-service-backup auth-server-down** command.
- When the VAP type is distributed-AP backup service, the backup VAP continuously detects the signal output of the distributed VAP with the same SSID. If the signal from the distributed VAP with the same SSID is not detected within 25 Beacon intervals, the backup VAP considers the distributed AP faulty and automatically releases signals to ensure that STAs can access the network. After the distributed VAP recovers, the signal of the backup VAP is shut down, and STAs are switched back to the distributed VAP.

Precautions

- After the VAP type is configured in the VAP profile view, the VAPs generated by the VAP profile use the configured VAP type. The new VAP type will overwrite the old one.
- For an AP management VAP:
  - Portal, MAC address, and 802.1X authentication using an external server is not supported.
  - The VAP profile in which the VAP type is set to **ap-management** can be applied only to one radio of an AP or AP group.
  - If an AD9431DN-24X or AirEngine 9700D-M is used as the central AP, STAs log in to RUs through the offline management VAP. If a central AP other than the AD9431DN-24X or AirEngine 9700D-M is used, STAs log in to the central AP through the offline management VAP.
- For an AP-offline backup service VAP:
  - Only the WPA3 SAE, WPA2-WPA3 PSK-SAE, open, WEP, WPA+PSK, WPA2+PSK and WPA-WPA2+PSK authentication modes are supported.
  - Service data can be forwarded only in direct mode.
  - When the number of configured AP-offline backup service VAPs reaches the maximum on the AP, if the offline management VAP function is enabled, the offline management VAP does not take effect when the AP goes offline.
- For an authentication-server-down backup service VAP:
  - Only the WPA3 SAE, WPA2-WPA3 PSK-SAE, open, WEP, WPA+PSK, WPA2+PSK and WPA-WPA2+PSK authentication modes are supported.
  - This VAP type is exclusive with the AP management VAP and AP-offline backup service VAP.
- For a distributed-AP backup service VAP:
  - Before configuring distributed AP backup, run the **distribute-mode enable** command to enable DAP network collaboration.
  - When a STA switches between a distributed VAP and backup VAP, the process is similar to WLAN roaming, and a few packets may be lost.

Example

Create the VAP profile **vap1** and set the VAP type to AP management VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] type ap-management
```

Create the VAP profile **vap1** and set the VAP type to **authentication-server-down backup service**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] type service-backup auth-server-down radius-server template temp1
```

11.1.172 u-apsd enable

Function

The **u-apsd enable** command enables the Unscheduled Automatic Power Save Delivery (U-APSD) function.

The **undo u-apsd enable** command disables the U-APSD function.

By default, the U-APSD function is disabled.

Format

u-apsd enable

undo u-apsd enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

U-APSD is a new energy saving mode defined for WMM, which can improve the energy-saving capability of STAs.

If some STAs on the network do not support the U-APSD function, disable the U-APSD function.

Precautions

The U-APSD function takes effect only when WMM is enabled.

After the U-APSD function is enabled, services may be interrupted.

Example

Enable the U-APSD function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] u-apsd enable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.173 undo ap

Function

The **undo ap** command deletes an AP.

Format

undo ap { **ap-name** *ap-name* | **ap-id** *ap-list* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Deletes the AP with a specified AP name.	The AP name must exist.
ap-id *ap-list*	Deletes APs with the specified IDs in a batch.	The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) or hyphens (-) to separate AP IDs. For example, **5,8,10-13,20** indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.
ap-mac *ap-mac*	Deletes the AP with a specified MAC address.	The AP's MAC address must exist.
ap-group *group-name*	Deletes the APs in a specified AP group.	The AP group must exist.
all	Deletes all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you do not want a specified Fit AP to go online on the AC, run this command to delete the Fit AP from the AC. After the Fit AP is deleted, it goes offline from the AC.

Configuration Impact

Deleting an AP will interrupt services of STAs connected to the AP.

Precautions

APs that are being upgraded, stay in standby or unauth state, or are executing the **ap-ping** command cannot be deleted.

In NETCONF mode, if any of the APs managed by the switch has been registered on the iMaster NCE-Campus, you cannot delete all APs using the **undo ap all** command. AP registration on the iMaster NCE-Campus indicates that an AP has been online on the iMaster NCE-Campus or the switch successfully synchronizes the configured AP information to the iMaster NCE-Campus.

Example

Delete the AP named **Area_1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] undo ap ap-name Area_1
Warning: Deleting the AP will interrupt user services. Continue?[Y/N]:y
```

11.1.174 untagged vlan (soft GRE profile view)

Function

The **untagged vlan** command configures soft GRE tunnel packets sent by APs not to carry VLAN tags.

The **undo untagged vlan** command restores the default status of whether soft GRE tunnel packets sent by APs carry VLAN tags.

By default, soft GRE tunnel packets sent by APs carry VLAN tags.

Format

untagged vlan *vlan-id*

undo untagged vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN tag to be removed.	The value is an integer that ranges from 1 to 4094.

Views

Soft GRE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving service data packets from STAs, an AP adds a service VLAN tag to the packets and performs soft GRE tunnel encapsulation. Then the soft GRE tunnel packets sent by the AP carry the VLAN tag. However, in some scenarios, the peer device of the soft GRE tunnel connected to the AP cannot process tagged packets. After this command is run, the soft GRE interface is added to the configured VLAN in untagged mode, and the PVID is also set to the configured VLAN. If the configured VLAN is a service VLAN, the service VLAN tag is removed after packets pass through the soft GRE interface. The soft GRE tunnel packets sent by the AP are transmitted in untagged mode.

Precautions

A soft GRE profile supports only one untagged VLAN.

Example

Configure APs to remove service VLAN 101 from soft GRE tunnel packets and transmit the packets in untagged mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] softgre-profile name soft1
[HUAWEI-wlan-softgre-prof-soft1] untagged vlan 101
```

11.1.175 utmost-power

Function

The **utmost-power disable** command disables radios from sending packets at the maximum power.

The **utmost-power enable** command enables radios to send packets at the maximum power.

The **undo utmost-power** command restores the adaptive mode for radios to send packets.

By default, a radio sends packets in adaptive mode.

Format

utmost-power { **disable** | **enable** }

undo utmost-power

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is valid for all country codes. You can run the **utmost-power enable** command to enable radios to send packets at the maximum power or run the **utmost-power disable** command to enable radios to send packets at the power specified by the country code. After you run the **undo utmost-power** command to restore the adaptive mode, radios send packets at the maximum power if the country code is CN or at the power specified by other country codes.

Precautions

This function may cause AP radios to exceed the laws and regulations of the local country or region. Therefore, ensure that you have obtained permission from the local administrative department before using this function.

For APs running R024C00 or later, this function takes effect only on the 2.4 GHz and 5 GHz radios, but not on 6 GHz radios.

Example

Disable radios from sending packets at the maximum power.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] utmost-power disable
```

11.1.176 vap-profile (WLAN view)

Function

The **vap-profile** command creates a VAP profile and displays the VAP profile view, or displays the view of an existing VAP profile.

The **undo vap-profile** command deletes a VAP profile.

By default, the system provides the VAP profile **default**.

Format

vap-profile name *profile-name*

undo vap-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a VAP profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all VAP profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a radio profile is bound to an AP, the AP can send and receive radio signals. After a VAP profile is bound to an AP, the VAP is generated to provide wireless access services for STAs. You can configure parameters in the VAP profile to enable APs to provide different wireless services.

Follow-up Procedure

Run the **vap-profile** command to apply the VAP profile in the AP group view, AP view, AP radio view, or AP group radio view so that the VAP profile can take effect.

Precautions

- The VAP profile **default** cannot be deleted.
- The VAP profile referenced in the AP group view, AP view, AP radio view, or AP group radio view cannot be deleted. To delete the VAP profile, unbind it from the AP group view, AP view, AP radio view, or AP group radio view first.
- By default, the SSID profile **default**, security profile **default**, and traffic profile **default** are bound to a VAP profile.

Example

Create the VAP profile **vap1** and enter the VAP profile view.

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



```
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1]
```

11.1.177 vap-profile

Function

The **vap-profile** command binds a VAP profile to a radio.

The **undo vap-profile** command unbinds a VAP profile from a radio.

By default, no VAP profile is bound to a radio.

Format

vap-profile *profile-name* **wlan** *wlan-id* **radio** { *radio-id* | **all** } [**service-vlan** { **vlan-id** *vlan-id* | **vlan-pool** *pool-name* }]

undo vap-profile *profile-name* **wlan** *wlan-id* **radio** { *radio-id* | **all** }

The parameter **radio** { *radio-id* | **all** } is supported only in the AP group view and AP view.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a VAP profile.	The VAP profile must exist.

Parameter	Description	Value
wlan *wlan-id*	Specifies the WLAN ID of a VAP.	The value is an integer that ranges from 1 to 16. **NOTE** • The WLAN ID for the WDS service can be 13 or 14. • The WLAN ID for the Mesh service is 16. • The WLAN ID for the offline management VAP configuration is 15 or an integer that ranges from 1 to 12. • For some AP models, the maximum number of VAPs supported by each radio is less than 16. If the value of *wlan-id* exceeds the AP specifications, the configuration cannot take effect and the AP cannot generate radio signals.
radio	Specifies a radio.	-
radio-id	Specifies a radio ID.	The value is an integer that ranges from 0 to 2.
all	Specifies all radios.	-
service-vlan	Specifies a service VLAN ID.	-
vlan-id *vlan-id*	Specifies a VLAN ID.	The VLAN ID must exist.
vlan-pool *pool-name*	Specifies the name of a VLAN pool.	The VLAN pool must exist.

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VAP profile using the **vap-profile (WLAN view)** command, bind it to a radio so that the VAP profile can take effect.

In some scenarios, users want to configure one VAP for all APs. However, APs use different service VLANs. To simplify the configuration, you can specify a service VLAN using the parameter **service-vlan** when binding a VAP profile. The priority of the service VLAN specified in this command is higher than that of a service VLAN configured using the **service-vlan** command.

Precautions

After a VAP profile is bound to a radio, parameter settings in the VAP profile apply to the radio using the profile.

Example

Create the VAP profile **vap1** and bind **vap1** to the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] vap-profile vap1 wlan 1 radio 0
```

11.1.178 vap-service-backup auth-server-down

Function

The **vap-service-backup auth-server-down** command manually enables or disables an authentication-server-down backup service VAP.

Format

vap-service-backup auth-server-down { **active** | **inactive** } [**vap-profile** *profile-name*]

Parameters

Parameter	Description	Value
active	Manually enables an authentication-server-down backup service VAP.	-
inactive	Manually disables an authentication-server-down backup service VAP.	-

Parameter	Description	Value
vap-profile *profile-name*	Specifies the name of a VAP profile. If this parameter is not specified, VAPs of this type on all referenced radios are enabled.	The VAP profile name must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an authentication-server-down backup service VAP is not automatically disabled after the authentication server is restored, the administrator can manually disable this VAP. When the authentication server rejects access of STAs, the administrator can manually enable an authentication-server-down backup service VAP to enable the STAs to enter the survival state.

Precautions

After an authentication-server-down backup service VAP is manually disabled, STAs associated with this VAP go offline.

Example

Manually enable an authentication-server-down backup service VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-service-backup auth-server-down active vap-profile vap1
```

11.1.179 vht a-mpdu max-length-exponent

Function

The **vht a-mpdu max-length-exponent** command sets the maximum length of an aggregated MPDU (A-MPDU) on the 802.11ac radio. MPDU stands for MAC protocol data unit.

The **undo vht a-mpdu max-length-exponent** command restores the maximum length of an A-MPDU on the 802.11ac radio to the default value.

By default, the index for the maximum length of an A-MPDU is 7. The maximum length of the A-MPDU is 1048575 bytes.

The function is not supported by the following models.

- AirEngine series APs

Format

vht a-mpdu max-length-exponent *max-length-exponent-index*

undo vht a-mpdu max-length-exponent

Parameters

Parameter	Description	Value
max-length-exponent-index	Indicates the index for the maximum length of the A-MPDU.	The value is an integer that ranges from 0 to 7. ● 0: indicates that the maximum length of the A-MPDU is 8191 bytes. ● 1: indicates that the maximum length of the A-MPDU is 16383 bytes. ● 2: indicates that the maximum length of the A-MPDU is 32767 bytes. ● 3: indicates that the maximum length of the A-MPDU is 65535 bytes. ● 4: indicates that the maximum length of the A-MPDU is 131071 bytes. ● 5: indicates that the maximum length of the A-MPDU is 262143 bytes. ● 6: indicates that the maximum length of the A-MPDU is 524287 bytes. ● 7: indicates that the maximum length of the A-MPDU is 1048575 bytes.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce costs, 802.11ac uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

Set the index of the maximum length of the A-MPDU to 2 in the 5G radio profile **default**. The index 2 corresponds to a maximum length of 32767 bytes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] vht a-mpdu max-length-exponent 2
```

11.1.180 a-msdu enable

Function

The **a-msdu enable** command enables the function of sending 802.11 frames in A-MSDU mode.

The **undo a-msdu** command restores the default configuration of sending 802.11 frames in A-MSDU mode.

By default, the function of sending 802.11 frames in A-MSDU mode is in self-adaptive state.

Format

a-msdu { **enable** | **disable** | **auto** }

undo a-msdu

Parameters

Parameter	Description	Value
enable	Enables the A-MSDU function.	-
disable	Disables the A-MSDU function.	-

Parameter	Description	Value
auto	Sets the A-MSDU function to the self-adaptive mode to enable or disable the A-MSDU function based on the AP capability. When this parameter is delivered to APs running a version earlier than V200R020C00, this function is disabled on the APs. When this parameter is delivered to APs running V200R020C00 or later, this function is enabled on the APs.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Aggregated MAC Service Data Unit (A-MSDU) technology aggregates multiple MAC Service Data Units (MSDUs) into an MAC Protocol Data Unit (MPDU), which reduces MAC layer costs of the 802.11 packets and improves packet transmission efficiency especially when short MSDUs are aggregated.

Precautions

The function of sending 802.11 frames in A-MSDU mode can be enabled on radios in compliance with 802.11n and later standards.

For AirEngine series APs, it is recommended that this function be enabled to improve air interface performance.

Example

Enable the function of sending 802.11 frames in A-MSDU mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] a-msdu enable
```

11.1.181 vht a-msdu max-frame-num

Function

The **vht a-msdu max-frame-num** command sets the maximum number of subframes that can be aggregated into an A-MSDU at one time.

The **undo vht a-msdu max-frame-num** command restores the default maximum number of subframes that can be aggregated into an A-MSDU at one time.

By default, a maximum of two subframes can be aggregated into an A-MSDU at one time.

The function is not supported by the following models.

- AirEngine series APs

Format

vht a-msdu max-frame-num *max-frame-number*

undo vht a-msdu max-frame-num

Parameters

Parameter	Description	Value
max-frame-number	Specifies the maximum number of subframes that can be aggregated into an A-MSDU at one time.	The value is an integer that ranges from 2 to 15.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A-MSDU technology aggregates multiple MSDUs into an MPDU, which reduces MAC layer costs of the 802.11 packets.

- When the wireless network quality is satisfactory, increase the maximum number of subframes that can be aggregated into an A-MSDU at one time to improve the network usage efficiency and wireless service performance.
- When the wireless network quality is unsatisfactory or delay-sensitive services, such as voice services are transmitted, reduce the maximum number of subframes that can be aggregated into an A-MSDU at one time to minimize the impact of packet loss on services and reduce packet transmission delay. Some STAs have restrictions on the number of subframes aggregated into a received A-MSDU. If the number of subframes sent by the AP exceeds the threshold, the STAs cannot receive the frames properly.

Prerequisites

The function of sending 802.11 frames in A-MSDU mode has been enabled using the **a-msdu enable** command.

Example

Set the maximum number of subframes that can be aggregated into an A-MSDU at one time to 3.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] vht a-msdu max-frame-num 3
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.182 vht mcs-map

Function

The **vht mcs-map** command configures the maximum number of spatial streams and the maximum MCS value supported by 802.11ac in the 5G radio profile.

The **undo vht mcs-map** command restores the default configuration.

By default, the maximum number of spatial streams and the maximum MCS value are not specified in the 5G radio profile.

Format

vht mcs-map nss *nss-value* **max-mcs** *max-mcs-value*

undo vht mcs-map

Parameters

Parameter	Description	Value
nss *nss-value*	Specifies the maximum number of available spatial streams.	The value is an integer ranging from 1 to 8.
max-mcs *max-mcs-value*	Specified the maximum MCS value that can be negotiated for spatial streams.	The value is an integer ranging from 7 to 9.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Rates of 802.11ac APs depend on the index value of MCS. A larger MCS value indicates a higher transmission rate.

- When *nss-value* is greater than or equal to the maximum number of spatial streams supported by an AP, the number of available spatial streams is the same as the maximum number of spatial streams supported by the AP.
- When *nss-value* is smaller than the maximum number of spatial streams supported by an AP, the number of available spatial streams is the same as *nss-value* and remaining spatial streams do not take effect.

  For example, if *nss-value* is set to 2 and the AP supports a maximum of 3 spatial streams, the maximum number of available spatial streams on the AP is 2.

Precautions

The following configurations take effect in descending order of priority: Reliability-first service guarantee mode configured using the **service-guarantee reliability-first** command in the SSID profile > Number of spatial streams and MCS value configured using the **vht mcs-map (SSID Profile)** command in the SSID profile > Number of spatial streams and MCS value configured using the **vht mcs-map** command in the 5G radio profile.

This configuration takes effect only when the AP communicates with STAs through 802.11ac.

Example

In the 5G radio profile, set the maximum number of available spatial streams to 2 and the maximum MCS value to 8.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] vht mcs-map nss 2 max-mcs 8
```

11.1.183 vht mcs-map (SSID profile)

Function

The **vht mcs-map** command configures the maximum number of spatial streams and the maximum MCS value supported by 802.11ac in the SSID profile.

The **undo vht mcs-map** command restores the default configuration.

By default, the maximum number of spatial streams and the maximum MCS value are not specified in the SSID profile.

Format

vht { **tx** | **rx** } **mcs-map nss** *nss-value* **map** *mcs-value*

undo vht { **tx** | **rx** } **mcs-map**

Parameters

Parameter	Description	Value
tx	Indicates the sent data.	-
rx	Indicates the received data.	-
nss *nss-value*	Specifies the maximum number of available spatial streams.	The value is an integer that ranges from 1 to 8.
map *mcs-value*	Specified the maximum MCS value that can be negotiated for spatial streams.	The value is an integer that ranges from 7 to 9.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Rates of 802.11ac APs depend on the index value of MCS. A larger MCS value indicates a higher transmission rate.

- When *nss-value* is greater than or equal to the maximum number of spatial streams supported by an AP, the number of available spatial streams is the same as the maximum number of spatial streams supported by the AP.
- When *nss-value* is smaller than the maximum number of spatial streams supported by an AP, the number of available spatial streams is the same as *nss-value* and remaining spatial streams do not take effect.

  For example, if *nss-value* is set to 2 and the AP supports a maximum of 3 spatial streams, the maximum number of available spatial streams on the AP is 2.

Precautions

The following configurations take effect in descending order of priority: Reliability-first service guarantee mode configured using the **service-guarantee reliability-first** command in the SSID profile > Number of spatial streams and MCS value configured using the **vht mcs-map (SSID Profile)** command in the SSID profile > Number of spatial streams and MCS value configured using the **vht mcs-map** command in the 5G radio profile.

This configuration takes effect only when the AP communicates with STAs through 802.11ac.

Example

In the SSID profile, set the maximum number of available spatial streams to 2 and the maximum MCS value to 8.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] vht rx mcs-map nss 2 map 8
```

11.1.184 vip-user bandwidth reservation-ratio

Function

The **vip-user bandwidth reservation-ratio** command configures the percentage of bandwidth reserved for VIP users.

The **undo vip-user bandwidth reservation-ratio** command restores the default percentage of bandwidth reserved for VIP users.

The default percentage of bandwidth reserved for VIP users is 20%.

Format

vip-user bandwidth reservation-ratio *reservation-ratio*

undo vip-user bandwidth reservation-ratio

Parameters

Parameter	Description	Value
reservation-ratio	Specifies the percentage of bandwidth reserved for VIP users.	The value is an integer that ranges from 0 to 100, in percentage. The default value is 20.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Bandwidth reservation for VIP users enables VIP users to preferentially enjoy experience improvement brought by resource reservation in the case of air interface congestion. You can run this command to adjust the percentage of bandwidth reserved for VIP users based on radios. The reserved bandwidth is shared by all VIP users.

The specific improvement effect depends on factors such as the number of VIP users and service types. It is recommended that you set *reservation-ratio* to 75%

when the **proportion of the number of VIP users to the total number of users** is 50% or set the value to 50% when the proportion is 20%. You can adjust the value based on the site requirements.

Example

In the 2G radio profile **default**, set the percentage of bandwidth reserved for VIP users to 30%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] vip-user bandwidth reservation-ratio 30
```

11.1.185 wlan

Function

The **wlan** command displays the WLAN view.

Format

wlan

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before performing WLAN configurations, run the **wlan** command to enter the WLAN view. All WLAN configuration commands need to be used in the WLAN view or WLAN sub-view.

Example

Enter the WLAN view.

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

11.2 AP Management Configuration Commands

11.2.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.2.2 access-user syslog-restrain enable

Function

The **access-user syslog-restrain enable** command enables system log suppression.

The **undo access-user syslog-restrain enable** command disables system log suppression.

By default, system log suppression is enabled.

Format

access-user syslog-restrain enable

undo access-user syslog-restrain enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a STA passes authentication or successfully associates with the AP, the AP sends system logs to the NMS server. A system log contains MAC addresses of the STA, AC, and AP, AP and AC name and current time, and authentication result.

If a STA fails to associate with an AP or fails authentication, the STA attempts to go online continuously. The AP sends a large number of duplicate logs to the AC in a short period, which wastes resources and deteriorates system performance. To prevent this problem, enable system log suppression.

Example

Enable system log suppression.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain enable
```


11.2.3 access-user syslog-restrain period

Function

The **access-user syslog-restrain period** command sets the period of system log suppression.

The **undo access-user syslog-restrain period** command restores the default period of system log suppression.

By default, the period of system log suppression is 300s.

Format

access-user syslog-restrain period *period*

undo access-user syslog-restrain period

Parameters

Parameter	Description	Value
period	Specifies the period of system log suppression.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a STA is authenticated or successfully associates with an AP, the AP sends system logs to the NMS server. A system log contains the MAC addresses of the STA, AP, and AC, AP name, AC name, current time, and authentication result.

A STA retries continuously after it fails to associate with an AP or pass the authentication. When this occurs, the AC sends a large number of logs in a short time. This results in a high statistics failure rate and degrades the NMS performance. The system log suppression function reduces impact of such logs on the NMS. After the period of system log suppression is set, the AC will send only one system log to the NMS server during the suppression period, reducing the load on the server.

Example

Set the period of system log suppression to 600s.


```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain period 600
```

11.2.4 ac-list (AP view)

Function

The **ac-list** command configures an AC IPv4 address list for APs.

The **undo ac-list** command restores the AC IPv4 address list to the default value.

By default, no AC IPv4 address list is configured.

Format

ac-list *ipv4-address* &<1-4>

undo ac-list

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an AC.	The value is in dotted decimal notation.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to statically configure an AC IPv4 address list for APs.

In addition to the static configuration, APs can dynamically obtain an AC IP address list through DHCP or DNS. When an AP goes online, it sends Discovery Request unicast packets to all ACs' IP addresses that are statically or dynamically obtained. After receiving the Discovery Request packets, the ACs respond to the AP with a Discovery Response packet. Based on AC information such as the AP management capability, maximum number of access STAs, and IP address, the AP selects one AC to establish a CAPWAP tunnel. If the AP does not have the AC IP address list or receives no response to the Discovery Request packet, the AP broadcasts Discovery Request packets to discover ACs on the same network segment.

Precautions

After the configuration is delivered, restart the APs to make the configuration take effect.

Example

Set the AC's IPv4 address to 192.168.10.1 in the AP view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] ac-list 192.168.10.1
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.5 ac-list (AP provisioning view)

Function

The **ac-list** command configures an AC IPv4 address list for APs.

The **undo ac-list** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, no AC IPv4 address list is configured.

Format

ac-list *ipv4-address* &<1-4>

undo ac-list

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an AC.	The value is in dotted decimal notation.

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to statically configure an AC IPv4 address list for APs.

In addition to the static configuration, APs can dynamically obtain an AC IP address list through DHCP or DNS. When an AP goes online, it sends Discovery

Request unicast packets to all ACs' IP addresses that are statically or dynamically obtained. After receiving the Discovery Request packets, the ACs respond to the AP with a Discovery Response packet. Based on AC information such as the AP management capability, maximum number of access STAs, and IP address, the AP selects one AC to establish a CAPWAP tunnel. If the AP does not have the AC IP address list or receives no response to the Discovery Request packet, the AP broadcasts Discovery Request packets to discover ACs on the same network segment.

Follow-up Procedure

Run the **commit** command to deliver configuration to APs and restart the APs to make the configuration take effect.

Example

Set the AC's IPv4 address to 192.168.10.1 in the AP provisioning view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] ac-list 192.168.10.1
```

11.2.6 address-mode (AP view)

Function

The **address-mode** command sets the mode in which an AP obtains an IP address.

The **undo address-mode** command restores the default mode in which an AP obtains an IP address.

By default, the mode in which an AP obtains an IP address is not configured.

Format

address-mode { **dhcp** | **static** }

undo address-mode

Parameters

Parameter	Description	Value
dhcp	Indicates that an IP address is obtained in DHCP mode. The AP functions as a DHCP client and is assigned an IP address by the DHCP server.	-
static	Indicates that a static IP address is obtained. The AP must be configured with a static IP address.	-

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **address-mode** command to configure an AP to obtain an IP address in DHCP or static mode.

Precautions

After the configuration is delivered, restart the APs to make the configuration take effect.

Example

Configure an AP to obtain an IP address in DHCP mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] address-mode dhcp
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.7 address-mode (AP provisioning view)

Function

The **address-mode** command sets the mode in which an AP obtains an IP address.

The **undo address-mode** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, the mode in which an AP obtains an IP address is not configured.

Format

address-mode { **dhcp** | **static** }

undo address-mode

Parameters

Parameter	Description	Value
dhcp	Indicates that an IP address is obtained in DHCP mode. The AP functions as a DHCP client and is assigned an IP address by the DHCP server.	-

Parameter	Description	Value
static	Indicates that a static IP address is obtained. The AP must be configured with a static IP address.	-

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **address-mode** command to configure an AP to obtain an IP address in DHCP or static mode.

Follow-up Procedure

Run the **commit** command to deliver configuration to APs and restart the APs to make the configuration take effect.

Example

Configure an AP to obtain an IP address in DHCP mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] address-mode dhcp
```

11.2.8 alarm-restriction disable

Function

The **alarm-restriction disable** command disables alarm suppression for an AP.

The **undo alarm-restriction disable** command enables alarm suppression for an AP.

By default, alarm suppression is enabled for an AP.

Format

alarm-restriction disable

undo alarm-restriction disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If a STA cannot go online due to security type mismatch, UAC, or access user upper limit exceeding, the STA will automatically re-connect to the AP. During this period, the AP sends a large number of the same STA association failure alarms to the AC, which degrades the system performance.

To solve this problem, enable alarm suppression for the AP. The AP then does not report alarms repeatedly in the alarm suppression period, preventing alarm storms.

Example

Disable alarm suppression for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] alarm-restriction disable
```

11.2.9 alarm-restriction period

Function

The **alarm-restriction period** command configures the period of alarm suppression on an AP.

The **undo alarm-restriction period** command restores the default period of alarm suppression for an AP.

The default alarm suppression period is 60 seconds on an AP.

Format

alarm-restriction period *period*

undo alarm-restriction period

Parameters

Parameter	Description	Value
period	Specifies the period of alarm suppression for an AP.	The value is an integer that ranges from 10 to 300, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap alarm-restriction period** command to configure the period of alarm suppression for an AP. The AP reports an alarm only one time in the specified period if the alarm is repeatedly generated.

Example

Set the period of alarm suppression to 200 seconds for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] alarm-restriction period 200
```

11.2.10 ap lldp enable

Function

The **ap lldp enable** command enables the Link Layer Discovery Protocol (LLDP) in the WLAN view.

The **undo ap lldp enable** command disables LLDP in the WLAN view.

By default, LLDP is enabled in the WLAN view.

Format

ap lldp enable

undo ap lldp enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LLDP is a Layer 2 discovery protocol defined in the IEEE 802.1ab standard. Using LLDP, the AC or NMS can obtain Layer 2 information about the connected APs, including APs' interfaces and connections with other devices. Additionally, the AC or NMS can obtain details about network topology and interface changes. To view the Layer 2 link status between APs, and between APs and switch or analyze the network topology, enable WLAN LLDP.

Precautions

WLAN LLDP can be enabled in the system view and the AP wired port link profile view.

- An AP can send and receive LLDP packets only after LLDP is enabled in both the WLAN view and the AP wired port link profile view.
- After LLDP is disabled in the WLAN view, the commands for enabling and disabling LLDP on the AP wired port link profile view do not take effect.

Example

Enable LLDP in the WLAN view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap lldp enable
```

11.2.11 ap manufacturer-config

Function

The **ap manufacturer-config** command restores the factory settings of APs.

Format

ap manufacturer-config { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of the AP whose factory settings need to be restored.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP whose factory settings need to be restored.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP whose factory settings need to be restored.	The AP ID must already exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

When a configuration error occurs on an AP, you can run this command to clear AP configurations.

NOTICE

Restoring the factory defaults of an AP will reset the AP and restore all the default AP configurations.

Example

Restore the factory settings of AP **N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap manufacturer-config ap-name N1-2
Warning: Reset AP to the manufacturing default configuration, continue?[Y/N]:y
```

11.2.12 ap update ftp-server

Function

The **ap update ftp-server** command configures basic FTP information, including the IP address, user name, and password of the FTP server.

The **undo ap update ftp-server** command restores default FTP settings.

By default, no basic FTP information is configured.

Format

ap update ftp-server ip-address *server-ip-address* [**port** *port*] **ftp-username** *ftp-username* **ftp-password cipher** *ftp-password*

undo ap update ftp-server ip-address

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies an IPv4 address for the FTP server.	The value is in dotted decimal notation.

Parameter	Description	Value
port *port*	Specifies a port number for the FTP server. If no port number is specified, the default port 21 is used.	The value is an integer that ranges from 1 to 65535.
ftp-username *ftp-username*	Specifies the user name for logging in to the FTP server.	The value is a string of 1 to 31 characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (") or spaces.
ftp-password	Specifies the password for logging in to the FTP server.	-
cipher	Specifies the password in ciphertext.	-
ftp-password	Specifies the FTP server password.	The value is a string of characters without question marks (?), and cannot start or end with double quotation marks (") or spaces. *ftp-password* can be a string of 1 to 188 characters in ciphertext, such as **%^%#A<g;&zQR7P3TF+,[MxQ1X%4[2~Gb]Vp#(e<y:~)/%^%#**, or a string of 1 to 128 characters in plaintext, such as **YsHsjx_202206**.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- The FTP configuration is used when the automatic upgrade and online upgrade modes are FTP. In the automatic upgrade or online upgrade, the AC sends basic FTP information to the AP, and the AP requests the FTP server for upgrade based on FTP information.
- After running the **ap update ftp-server** command, you can perform the following operations:
  a. Run the **ap update mode** command to set the upgrade mode to ftp-mode.
  b. Run the **ap update multi-load** command to upgrade APs in batches.

Precautions

- It is recommended that you use an external FTP server to upgrade APs. If the AC functions as the FTP server, a maximum of five APs can be upgraded simultaneously. If there are *n* login VTY users, the maximum number of APs that can be upgraded simultaneously is subtracted by *n* - 1.
- APs do not support the double quotation marks ("). Ensure that the FTP server user name and unencrypted password configured on the AC do not contain the preceding characters. Otherwise, the FTP upgrade fails.
- When the FTP port number is specified, the upgrade is applicable only to APs in V200R020C10 and later. If the source version of APs is earlier than V200R020C10, the FTP upgrade fails.
- The FTP server must support the REST field. Otherwise, the upgrade will fail. If the following information is displayed, the upgrade fails because the server does not support the REST field. In this case, replace the server.
  Error: Upgrade failed because the FTP server does not support the REST command.

Example

Configure the IP address, user name, and password of the FTP server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update ftp-server ip-address 192.168.1.100 ftp-username admin ftp-password cipher YsHsjx_202206
```

11.2.13 ap update ftp-server max-connect-number

Function

The **ap update ftp-server** command configures the maximum number of APs that can be upgraded simultaneously in FTP mode.

The **undo ap update ftp-server** command restores the default maximum number of APs that can be upgraded simultaneously in FTP mode.

By default, a maximum of 50 APs can be upgraded simultaneously in FTP mode.

Format

ap update ftp-server max-connect-number *max-connect-number*

undo ap update ftp-server max-connect-number

Parameters

Parameter	Description	Value
max-connect-number	Specifies the maximum number of APs that can be upgraded simultaneously.	The value is an integer that ranges from 1 to 64.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When APs are upgraded in FTP mode, you can configure the value of *max-connect-number* to change the maximum number of APs that can be upgraded simultaneously.

- If the number of APs to be upgraded is equal to or smaller than *max-connect-number*, all APs can be upgraded simultaneously.
- If the number of APs to be upgraded is larger than *max-connect-number*, only the specified number of APs can be upgraded simultaneously. After the specified number of APs are upgraded, the remaining APs are upgraded automatically until all APs are upgraded. The number of APs that are upgraded at a time cannot exceed the value of *max-connect-number*.

Precautions

An external FTP server can be used, which is recommended. The AC can also function as the FTP server.

- When an external FTP server is used, the maximum number of APs that can be upgraded simultaneously is the configured *max-connect-number*.
- If an AC is used as the FTP server, a maximum of five APs can be upgraded simultaneously even if the specified number is larger than five.

  When the AC functions as the FTP server, run the **ap update ftp-server max-connect-number** *max-connect-number* command to set the maximum number of APs that can be upgraded simultaneously. The value of *max-connect-number* is an integer ranging from 1 to 5. During the upgrade, a maximum of 1 to 5 APs can be upgraded at a time until all APs are upgraded.

  If the configured number of APs to be upgraded simultaneously is larger than five, an error message will be displayed after the first five APs are upgraded. The remaining APs cannot be automatically upgraded. You have to repeat the command until all APs are upgraded.

If there are *n* login VTY users, the maximum number of APs that can be upgraded simultaneously is subtracted by *n* - 1.

Example

Set the maximum number of APs that can be upgraded simultaneously in FTP mode to 10.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update ftp-server max-connect-number 10
```

11.2.14 ap update load

Function

The **ap update load** command upgrades a specified AP.

The **undo ap update load** command cancels AP upgrade.

Format

ap update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } **update-filename** *update-file-name*

undo ap update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of the AP to be upgraded.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP to be upgraded.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP to be upgraded.	The AP ID must already exist.
update-filename *update-file-name*	Specifies the AP upgrade file.	The upgrade file name must already exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When APs are upgraded in batches based on AP types, if the new version fails, the version rollback takes a long period. Therefore, you can upgrade a single AP to check whether faults occur on the version, ensuring successful upgrades in batches.

Prerequisites

When the AC mode is used, the AP upgrade file has been uploaded to the AC. If the FTP or SFTP mode is used, the AP upgrade file has been uploaded to the FTP server or SFTP server.

The AP is in normal or vmiss state.

Follow-up Procedure

Run the **ap update reset** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } command to restart the AP to make the upgrade take effect.

Precautions

The **undo ap update load** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } command cancels AP upgrade. However, if the AP system software has been written to the flash memory during the upgrade, the command does not take effect. You can run the **display ap update status** { **ap-name** *ap-name* | **ap-id** *ap-id* } command to check AP upgrade progress.

Example

Upgrade the AP **N1-2** using the upgrade file **AirEngineX760-V200R021C10.cc**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update load ap-name N1-2 update-filename AirEngineX760-V200R021C10.cc
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP or SFTP upgrade mode is recommended. Continue? [Y/N]:y
```

11.2.15 ap update mode

Function

The **ap update mode** command configures the AP upgrade mode.

The **undo ap update mode** command restores the default AP upgrade mode.

The default upgrade mode is **ac-mode**.

Format

ap update mode { **ftp-mode** | **ac-mode** | **sftp-mode** }

undo ap update mode

Parameters

Parameter	Description	Value
ac-mode	Indicates the AP upgrade mode in which APs download the upgrade version file from the AC.	-
ftp-mode	Indicates the FTP mode. The AC delivers the FTP configuration to APs using the **ap update ftp-server** command, and APs download the upgrade version file from the FTP server.	-
sftp-mode	Indicates the SFTP mode. The AC delivers the SFTP configuration to APs using the **ap update sftp-server** command, and APs download the upgrade version file from the SFTP server.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

- The AC, FTP, or SFTP upgrade mode must be preset on the AP for automatic upgrade and online upgrade.
- Subsequently, you can run the **ap update multi-load** command to upgrade APs in batches.

NOTE

SFTP is recommended because it is more secure than FTP.

Example

Set the AP upgrade mode to **sftp-mode**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update mode sftp-mode
```

11.2.16 ap update multi-load

Function

The **ap update multi-load** command upgrades APs in batches.

The **undo ap update multi-load** command cancels batch upgrade of APs.

Format

ap update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

ap update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

undo ap update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

undo ap update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies the AP type ID.	The value is an integer that ranges from 0 to .
ap-group *group-name*	Specifies an AP group.	The AP group must exist.
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ap update multi-load ap-type** *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] command to upgrade APs of the same type in batches in the online upgrade mode.

- If **ap-group** *group-name* is specified, only APs of the same type and in the specified AP group are upgraded.
- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs of the specified type and with the specified AP name or AP ID are upgraded
- If none of the **ap-group** *group-name*, **ap-name** *ap-name*, and **ap-id** *ap-id* parameters are specified, all APs of the specified type are upgraded.

- If the type of APs specified by **ap-group** *group-name*, **ap-name** *ap-name*, or **ap-id** *ap-id* is different from **ap-type** *type-id*, the APs cannot be upgraded.

You can run the **ap update multi-load ap-group** *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] command to batch upgrade APs in the specified AP group online.

- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs with the specified name or ID in the specified AP group are upgraded.
- If neither **ap-name** *ap-name* nor **ap-id** *ap-id* is specified, all APs in the specified AP group are upgraded.
- If APs specified by **ap-name** *ap-name* and **ap-id** *ap-id* are in different AP groups, the APs cannot be upgraded.

Prerequisites

AP upgrade files have been configured in batches using the **ap update update-filename** command.

Follow-up Procedure

Run the **ap update multi-reset** command to reset APs in batches to make AP upgrade take effect.

Precautions

The **undo ap update multi-load** command cancels batch upgrade of APs. However, if the AP system software has been written to the flash memory during the upgrade, the command does not take effect. You can run the **display ap update status all** command to check AP upgrade progress.

Example

Upgrade APs with **type-id** 56 in batches online.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update multi-load ap-type 56
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP or SFTP upgrade mode is recommended. Continue? [Y/N]:y
```

Upgrade all APs in the AP group **group1** in batches online.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update multi-load ap-group group1
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP or SFTP upgrade mode is recommended. Continue? [Y/N]:y
```

11.2.17 ap update multi-reset

Function

The **ap update multi-reset** command resets APs in batches.

The **undo ap update multi-reset partition** command cancels the AP reset by channel-based partition.

Format

ap update multi-reset ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

ap update multi-reset ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

ap update multi-reset { **partition** { **all** | **partition-id** *partition-id* } | **ap-id** *ap-id* } [**primary-access** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* }]

undo ap update multi-reset partition

Parameters

Parameter	Description	Value
ap-type *type-id*	Resets APs of the specified type ID.	The AP type ID must exist.
ap-group *group-name*	Resets APs in the specified AP group.	The AP group must exist.
ap-name *ap-name*	Resets the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Resets the AP with a specified ID.	The AP ID must exist.
partition all	Resets APs in all channel-based partitions.	-
partition partition-id *partition-id*	Resets APs in the specified channel-based partition.	The value is an integer that ranges from 0 to 255.
primary-access ipv4 *ipv4-address*	Specifies the IPv4 address of the AC with which APs re-establish links after the APs are reset.	The value is in dotted decimal notation.
primary-access ipv6 *ipv6-address*	Specifies the IPv6 address of the AC with which APs re-establish links after the APs are reset.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

This command resets APs in batches and can be used only after APs are upgraded in batches.

Run the **ap update multi-reset ap-type** *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] command to batch reset APs of the specified type online.

- If **ap-group** *group-name* is specified, only APs of the specified type and in the specified AP group are reset.
- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs of the specified type and with the specified AP name or ID are reset.
- If none of the **ap-group** *group-name*, **ap-name** *ap-name*, and **ap-id** *ap-id* parameters are specified, all APs of the specified type are reset.
- If the type of APs specified by **ap-group** *group-name*, **ap-name** *ap-name*, or **ap-id** *ap-id* is different from **ap-type** *type-id*, the APs cannot be reset.

You can run the **ap update multi-reset ap-group** *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] command to batch reset APs in the specified AP group online.

- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs with the specified name or ID in the specified AP group are reset.
- If neither **ap-name** *ap-name* nor **ap-id** *ap-id* is specified, all APs in the specified AP group are reset.
- If APs specified by **ap-name** *ap-name* or **ap-id** *ap-id* are not in the AP group specified by **ap-group** *group-name*, the APs cannot be reset.

The **ap update multi-reset** { **partition** { **all** | **partition-id** *partition-id* } | **ap-id** *ap-id* } [**primary-access** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* }] command is used to reset APs in a specified channel-based partition in batches. To perform an in-service upgrade for all APs on the entire network, you can divide APs into different partitions based on channels and reset the APs by partition in sequence after loading the target version files to all APs. This prevents network service interruption caused by resetting a large number of APs. When APs are reset by partition, surrounding APs automatically fill coverage holes to ensure service continuity. For service continuity, ensure that at least two APs are deployed in one place.

In dual-AC scenarios, when APs are upgraded by channel-based partition, you can specify the IP address of the AC with which APs re-establish links after the APs are reset.

If an upgrade exception occurs when the **ap update multi-reset partition all** command is used to reset all RUs by channel-based partition, you can run the **undo ap update multi-reset partition** command to cancel the subsequent RU reset by channel-based partition.

Example

Reset APs with **type-id** 56 in batches.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update multi-reset ap-type 56
Warning: Reset the APs in batches to make the upgrade take effect. Continue? [Y/N]:y
```


11.2.18 ap update reset

Function

The **ap update reset** command restarts a specified AP after it is upgraded.

Format

ap update reset { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of the AP to be restarted.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP to be restarted.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP to be restarted.	The AP ID must already exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After an AP has been upgraded, run the **ap update reset** command to restart it to make the AP upgrade take effect.

Prerequisites

The AP is in normal or vmiss state.

The **ap update load** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } **update-filename** *update-file-name* command has been executed to upgrade a specified AP, and the **display ap update status** command has been executed to verify that **Update Status** of the specified AP is **succeed(need reset)**.

Example

Restart AP **N1-2** after the upgrade.

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



```
[HUAWEI-wlan-view] ap update load ap-name N1-2 update-filename AirEngineX760-V200R021C10.cc
[HUAWEI-wlan-view] ap update reset ap-name N1-2
```

11.2.19 ap update sftp-server

Function

The **ap update sftp-server** command configures basic SFTP information, including the IP address, user name, and password of the SFTP server.

The **undo ap update sftp-server** command restores default SFTP settings.

By default, no basic SFTP information is configured.

Format

ap update sftp-server ip-address *server-ip-address* [**port** *port*] **sftp-username** *sftp-username* **sftp-password cipher** *sftp-password*

undo ap update sftp-server ip-address

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies an IPv4 address for the SFTP server.	The value is in dotted decimal notation.
port *port*	Specifies a port number for the SFTP server. If no port number is specified, the default port 22 is used.	The value is an integer that ranges from 1 to 65535.
sftp-username *sftp-username*	Specifies the user name for logging in to the SFTP server.	The value is a string of 1 to 31 characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (") or spaces.
sftp-password	Specifies the password for logging in to the SFTP server.	-
cipher	Specifies the password in ciphertext.	-

Parameter	Description	Value
sftp-password	Specifies the SFTP server password.	The value is a string of characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (") or spaces. *sftp-password* can be a string of 1 to 188 characters in ciphertext, such as **%^ %#A<g;&zQR7P3TF +,[MxQ1X %4[2~Gb]Vp#(e<y: ~)/%^%#**, or a string of 1 to 128 characters in plaintext, such as **YsHsjx_202206**.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- The SFTP configuration is used when the automatic upgrade and online upgrade modes are SFTP. In the automatic upgrade or online upgrade, the AC sends basic SFTP information to the AP, and the AP requests the SFTP server for upgrade based on SFTP information.
- After running the **ap update sftp-server** command, you can perform the following operations:
  a. Run the **ap update mode** command to set the upgrade mode to sftp-mode.
  b. Run the **ap update multi-load** command to upgrade APs in batches.

Precautions

- It is recommended that you use an external SFTP server to upgrade APs. If the AC functions as the SFTP server, a maximum of five APs can be upgraded simultaneously. If there are *n* login VTY users, the maximum number of APs that can be upgraded simultaneously is subtracted by *n* - 1.

- APs do not support the double quotation marks ("). Ensure that the SFTP server user name and unencrypted password configured on the AC do not contain the preceding characters. Otherwise, the SFTP upgrade fails.
- When the SFTP port number is specified, the upgrade is applicable only to APs in V200R020C10 and later. If the source version of APs is earlier than V200R020C10, the SFTP upgrade fails.

Example

Configure the IP address, user name, and password of the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update sftp-server ip-address 192.168.1.100 sftp-username admin sftp-password cipher YsHsjx_202206
```

11.2.20 ap update sftp-server max-connect-number

Function

The **ap update sftp-server** command configures the maximum number of APs that can be upgraded simultaneously in SFTP mode.

The **undo ap update sftp-server** command restores the default maximum number of APs that can be upgraded simultaneously in SFTP mode.

By default, a maximum of 50 APs can be upgraded simultaneously in SFTP mode.

Format

ap update sftp-server max-connect-number *max-connect-number*

undo ap update sftp-server max-connect-number

Parameters

Parameter	Description	Value
max-connect-number	Specifies the maximum number of APs that can be upgraded simultaneously.	The value is an integer that ranges from 1 to 64.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When APs are upgraded in SFTP mode, you can configure the value of *max-connect-number* to change the maximum number of APs that can be upgraded simultaneously.

- If the number of APs to be upgraded is equal to or smaller than *max-connect-number*, all APs can be upgraded simultaneously.
- If the number of APs to be upgraded is larger than *max-connect-number*, only the specified number of APs can be upgraded simultaneously. After the specified number of APs are upgraded, the remaining APs are upgraded automatically until all APs are upgraded. The number of APs that are upgraded at a time cannot exceed the value of *max-connect-number*.

Precautions

An external SFTP server can be used, which is recommended. The AC can also function as the SFTP server.

- When an external SFTP server is used, the maximum number of APs that can be upgraded simultaneously is the configured *max-connect-number*.
- When an AC is used as the SFTP server, a maximum of five APs can be upgraded simultaneously even if the specified number of APs to be upgraded is larger than five.

  When the AC functions as the SFTP server, run the **ap update sftp-server max-connect-number** *max-connect-number* command to set the maximum number of APs that can be upgraded simultaneously. The value of *max-connect-number* is an integer ranging from 1 to 5. During the upgrade, a maximum of 1 to 5 APs can be upgraded at a time until all APs are upgraded.

  If *max-connect-number* is set larger than 5, an error message will be displayed after the first five APs are upgraded. The remaining APs cannot be automatically upgraded. You have to repeat the command until all APs are upgraded.

  If there are *n* login VTY users, the maximum number of APs that can be upgraded simultaneously is subtracted by *n* - 1.

Example

Set the maximum number of APs that can be upgraded simultaneously in SFTP mode to 10.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update sftp-server max-connect-number 10
```

11.2.21 ap update update-filename

Function

The **ap update update-filename** command configures the upgrade file name for APs of a specified type.

The **undo ap update update-filename** command deletes the upgrade file name for APs of a specified type.

Format

ap update update-filename *filename* **ap-type** *type-id* [**ap-group** *ap-group-name*]

undo ap update update-filename ap-type *type-id* [**ap-group** *ap-group-name*]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies the AP type ID.	The value is an integer that ranges from 0 to .
filename	Specifies the AP upgrade file name.	The value is a string of 1 to 255 case-sensitive characters. Ensure that the file name is the same as the actual upgrade file name and has an extension.
ap-group *ap-group-name*	Specifies an AP group.	The AP group must already exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

If you specify **ap-group** *ap-group-name*, the command configures the upgrade file name only for APs of the specified type and in the specified group. The upgrade file name configured for an AP group takes precedence over that configured without an AP group specified if they are different. To cancel the upgrade file name configuration of the AP group, specify the AP group name using the parameter **ap-group** *ap-group-name* when running the **undo** command.

Run the **ap update multi-load ap-type** command to upgrade APs of the same type in batches.

Example

Set the upgrade file name for APs with the type ID 127 to **AirEngineX760-V200R021C10.cc**.

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



```
[HUAWEI-wlan-view] ap update update-filename AirEngineX760-V200R021C10.cc ap-type 127
Warning: If an AP is performing the automatic upgrade, the AP will be upgraded to the latest version.
Continue?[Y/N]:y
Warning: If AP update mode is AC-mode, update-file's default path is flash:/. Continue?[Y/N]:y
```

11.2.22 ap update schedule-task

Function

The **ap update schedule-task** command configures a scheduled AP upgrade task.

The **undo ap update schedule-task** command deletes a scheduled AP upgrade task.

By default, no scheduled AP upgrade task is configured.

Format

ap update schedule-task task-id *task-id* **start-time** *start-time start-date* **stop-time** *stop-time stop-date* **ap-type** *type-id* [**ap-group** *group-name* | { { **ap-name** *ap-name* } &<1-10> } | { { **ap-id** *ap-id* } &<1-10> }]

ap update schedule-task task-id *task-id* **start-time** *start-time start-date* **stop-time** *stop-time stop-date* **ap-group** *group-name*

undo ap update schedule-task { **all** | **task-id** *task-id* }

Parameters

Parameter	Description	Value
task-id *task-id*	Specifies the ID of a scheduled AP upgrade task.	The value is an integer that ranges from 0 to 31.
start-time *start-time*	Specifies the start time of the scheduled AP upgrade task.	The value is in HH:MM format, ranging from 00:00 to 23:59.
start-date	Specifies the start date of the scheduled AP upgrade task.	The value is in YYYY/MM/DD format, ranging from 2000-01-01 to 2050-12-31.
stop-time *stop-time*	Specifies the end time of the scheduled AP upgrade task.	The value is in HH:MM format, ranging from 00:00 to 23:59.

Parameter	Description	Value
stop-date	Specifies the end date of the scheduled AP upgrade task.	The value is in YYYY/MM/DD format, ranging from 2000-01-01 to 2050-12-31. *stop-time stop-date* must be later than *start-time start-date*.
ap-type *type-id*	Specifies an AP type ID.	The value is an integer. To view all AP types, run the **display ap-type all** command.
ap-group *group-name*	Specifies an AP group name.	The value is a string of 1 to 35 characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?) or slashes (/), and cannot start or end with spaces or double quotation marks (" "). If the AP group name contains spaces, the input name must start and end with a quotation mark ("), for example, **"hello name1"**. The quotation marks at the beginning and end of the AP group name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
ap-id *ap-id*	Specifies an AP ID.	The value is an integer. The value range depends on the actual device.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure a scheduled AP upgrade task to upgrade APs in a specified time period, such as off-peak hours.

If you specify **ap-group** *group-name* in the command, the configured task will upgrade only APs in the specified AP group. Similarly, if you specify **ap-type** *type-id*, **ap-name** *ap-name*, or **ap-id** *ap-id*, the configured task will upgrade only the specified APs.

The scheduled task configuration will not be automatically deleted after a scheduled upgrade task is completed. To delete the task, run the **undo ap update schedule-task** { **all** | **task-id** *task-id* } command.

Prerequisites

The AP upgrade file has been specified using the **ap update update-filename** command.

Configuration Impact

After scheduled upgrade tasks are configured, automatic upgrade cannot be performed if not all tasks are in the DONE, OVERTIME, or DEAD state. To perform automatic upgrade, you need to delete the scheduled upgrade tasks not in DONE, OVERTIME, or DEAD state. To check the status of scheduled AP upgrade tasks, run the **display ap update schedule-task** command.

Precautions

- For scheduled AP upgrade tasks with the same start time, the task with a smaller **task-id** *task-id* is executed preferentially.
- During the scheduled AP upgrade, if the time for task B is reached before task A is completed, task B waits until task A is completed. Subsequent scheduled AP upgrade tasks wait in sequence until the previous task is completed.
- When the time specified by **stop-time** *stop-time stop-date* is reached, ongoing upgrade tasks continue until the upgrade is completed and those tasks waiting in queues stop.
- After APs in a scheduled upgrade task are all upgraded, the APs automatically restart. The APs that fail the upgrade do not restart.
- After a scheduled AP upgrade task is configured, if the AP group or all APs are deleted, the task fails to be executed, which is not recorded as upgrade failure information.
- If an AP is performing the automatic upgrade when you configure a scheduled AP upgrade task, the upgrade continues until the upgrade is completed. APs that have not started the automatic upgrade will not execute the automatic upgrade.
- If the system time is changed after you configure a scheduled AP upgrade task, the following impacts may be caused:
  - If the system time is changed **before** the scheduled AP upgrade task starts, the start time and end time of the scheduled AP upgrade task are subject to the system time **after** the change. For example, the current system time is 1:00, and the start time and end time of the scheduled AP upgrade task are 3:00 and 4:00 respectively. When the system time is changed to 2:00 at 1:05, the start time and end time of the scheduled AP upgrade task are still 3:00 and 4:00 respectively.
  - If the system time is changed **after** the scheduled AP upgrade task starts, the start time and end time of the scheduled AP upgrade task are subject to the system time **before** the change.

Example

Configure APs with **ap-type** as **54** to perform the scheduled upgrade from 01:00 to 04:00 on May 20, 2018.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update schedule-task task-id 1 start-time 1:00 2018/5/20 stop-time 4:00 2018/5/20 ap-type 54
```

11.2.23 ap username

Function

The **ap username** command sets the user name and password for AP login.

By default, no user name or password is configured for AP login.

Format

ap username *username* **password cipher**

Parameters

Parameter	Description	Value
username	Specifies the user name for AP login.	The value is a string of 4 to 31 characters. It can contain letters, underscores, and digits, and must start with a letter.
password	Specifies the password for AP login.	-

Parameter	Description	Value
cipher	Indicates the ciphertext password.	The password can be entered in plaintext or ciphertext: • In plaintext, the password is a string of 8 to 128 case-sensitive characters. It must contain at least three of the following types: uppercase letters, lowercase letters, digits, and special characters, without question marks (?). • In ciphertext, the password is a string of 48 to 188 characters. It must contain at least the following types: uppercase letters, lowercase letters, digits, and special characters.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

You can run this command to change the user name and password for logging in to an AP. If the user name and password of the AP have not been configured, you must configure them first in order to log in to the AP.

Running this command will disconnect the administrator who is logging in to the AP.

NOTE

It is recommended that you change the user name and password in a timely manner to ensure device security.

The password cannot be the same as the user name or the mirror user name.

Example

Set the user name to **example** and password to **Zz123456**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap username example password cipher
Warning: This operation will disconnect administrator users logging in to the AP, Continue? [Y/N]:y
Enter the password (plain-text password of 8-128 characters or cipher-text password of 48-188 characters that must be a combination
of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):
Confirm password:
```

11.2.24 ap-group

Function

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

The **undo ap-group** command deletes an AP group.

By default, the system provides the AP group **default**.

Format

ap-group name *group-name*

undo ap-group { **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of an AP group.	The value is a string of 1 to 35 characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?) or slashes (/), and cannot start or end with spaces or double quotation marks (" "). If the AP group name contains spaces, the input name must start and end with a quotation mark ("), for example, **"hello name1"**. The quotation marks at the beginning and end of the AP group name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
all	Deletes all AP groups. **NOTE** This configuration does not delete the AP group **default** or any AP group that has APs in it.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same configuration on multiple APs, add the APs to an AP group and perform the configuration in the AP group. The configuration takes effect on all APs of the group. This prevents repetitive configuration.

Follow-up Procedure

Run the **ap-group (AP view)** or **ap-regroup** command to add APs to an AP group.

Precautions

- If the configuration of an AP in the AP view is different from that in the AP group view, the configuration in the AP view is preferentially used.
- The device supports a maximum of 256 AP groups.
- The AP group that has APs cannot be deleted. The AP group **default** cannot be deleted either.
- By default, an AP group has the following profiles bound: AP system profile **default**, 2G radio profile **default**, 5G radio profile **default**, regulatory domain profile **default**, WIDS profile **default**, and AP wired port profile **default**.

Example

Create the AP group **group1** and display the AP group view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1]
```

11.2.25 ap-group (AP view)

Function

The **ap-group** command configures an AP group.

The **undo ap-group** command restores the default AP group.

By default, no AP group is configured.

Format

ap-group *ap-group*

undo ap-group

Parameters

Parameter	Description	Value
ap-group	Specifies an AP group.	The AP group must exist.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same configuration on multiple APs, add the APs to an AP group and perform the configuration in the AP group. The configuration takes effect on all APs of the group. This prevents you from configuring each AP one by one.

Each AP must be added to an AP group. If no AP group is configured for an AP, the AP automatically joins the AP group **default**.

Example

Configure the AP group **ap-new-group** for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] ap-group ap-new-group
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, Whether to continue? [Y/N]:y
```

11.2.26 ap-group all vap-profile

Function

The **ap-group all vap-profile** command binds a VAP profile to all AP groups.

The **undo ap-group all vap-profile** command unbinds a VAP profile from all AP groups.

By default, no VAP profile is bound to radios of an AP group.

Format

ap-group all vap-profile *profile-name* **wlan** *wlan-id* **radio** { *radio-id* | **all** }

undo ap-group all vap-profile wlan *wlan-id* **radio** { *radio-id* | **all** }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a VAP profile.	The value must be the name of an existing VAP profile.

Parameter	Description	Value
wlan *wlan-id*	Specifies a VAP ID.	The value is an integer that ranges from 1 to 16. **NOTE** • The WLAN ID for the WDS service can be 13 or 14. • The WLAN ID for the Mesh service is 16. • The WLAN ID for the offline management VAP configuration is 15 or an integer that ranges from 1 to 12. • For some AP models, the maximum number of VAPs supported by each radio is less than 16. If the value of *wlan-id* exceeds the AP specifications, the configuration cannot take effect and the AP cannot generate radio signals.
radio *radio-id*	Specifies a radio ID.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: • AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 • AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T • AirEngine 8771-X1T
radio all	Specifies all radios.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap-group all vap-profile** command to bind a VAP profile to all AP groups.

Example

Bind the VAP profile **office01** to all AP groups.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group all vap-profile office01 wlan 1 radio 0
Info: This operation may take a few seconds, please wait.....done.
Warning: This operation is to bind the profile to 4 AP groups. Success count: 3. Failure count: 1. The failure
```



```
causes are as follows:
--------------------------------------------------------------------------------
AP group                    Config fail reason
--------------------------------------------------------------------------------
default                     The WLAN ID on the radio is in use. Please use an unassigned WLAN ID.
--------------------------------------------------------------------------------
```

Table 11-66 Description of the **ap-group all vap-profile** command output

Item	Description
AP group	AP group to which the VAP profile fails to be bound.
Config fail reason	Binding failure cause.

11.2.27 ap-group all wids-profile

Function

The **ap-group all wids-profile** command binds a WIDS profile to all AP groups.

The **undo ap-group all wids-profile** command unbinds a WIDS profile from all AP groups.

By default, the WIDS profile **default** is bound to an AP group.

Format

ap-group all wids-profile *profile-name*

undo ap-group all wids-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a WIDS profile.	The value must be the name of an existing WIDS profile.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap-group all wids-profile** command to bind a WIDS profile to all AP groups.

Example

Bind the WIDS profile **office01** to all AP groups.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group all wids-profile office01
```

11.2.28 ap-group all wired-port-profile

Function

The **ap-group all wired-port-profile** command binds an AP wired port profile to all AP groups.

The **undo ap-group all wired-port-profile** command unbinds an AP wired port profile from all AP groups.

By default, the AP wired port profile **default** is bound to an AP group.

Format

ap-group all wired-port-profile *profile-name interface-type interface-number*

undo ap-group all wired-port-profile *interface-type interface-number*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port profile.	The value must be the name of an existing AP wired port profile.
interface-type interface-number	Specifies the type and number of an AP's wired interface.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap-group all wired-port-profile** command to bind an AP wired port profile to all AP groups.

Example

Bind the AP wired port profile **office01** to all AP groups.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group all wired-port-profile office01 gigabitethernet 0
```

11.2.29 ap-mode

Function

The **ap-mode** command sets the working mode of an AP.

The **undo ap-mode** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, the working mode of an AP is not specified in the AP provisioning view.

Format

ap-mode { **fat** | **cloud** | **fit** }

undo ap-mode

Parameters

Parameter	Description	Value
fat	Specifies the Fat mode.	-
cloud	Specifies the cloud mode.	-
fit	Specifies the Fit mode.	-

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The working mode of an AP is configured on the AC and delivered to the AP. After a restart, the AP will switch the working mode accordingly.

Prerequisites

- The AP has gone online on the AC in Fit mode.
- Corresponding system files have been uploaded to the AC, FTP server, or SFTP server.

Follow-up Procedure

Run the **commit** command to commit the configuration.

In V200R023C00 or a later version: To switch the working mode of a Fit AP, run the **undo ap** (WLAN view) command on the to delete the Fit AP from the before the restart is complete. If the Fit AP is not deleted, the AP may switch back to the Fit mode in accordance with the foolproof mechanism after the restart is complete.

Configuration Impact

After the working mode of the AP is switched to Fat or cloud, the AP will be out of control by the AC.

NOTICE

This command is supported only by the following models:

- AirEngine series APs (excluding RUs) (The AirEngine 8771-X1T supports only the Fit and cloud modes.)
- AirEngine series central APs

Example

Set the working mode of an AP to Fat.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] ap-mode fat
Warning: When the configuration is committed, the AP mode will be switched if supported and the AP will be out of control by the AC.Continue?[Y/N]: y
```

11.2.30 ap-name

Function

The **ap-name** command displays the AP view.

Format

ap-name *ap-name*

Parameters

Parameter	Description	Value
ap-name	Specifies the AP name.	The AP name must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After entering the AP view, you can perform personalized configuration on an AP.

Example

Display the view of the AP named **area_1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-name area_1
[HUAWEI-wlan-ap-2]
```

11.2.31 ap-name (AP provisioning view)

Function

The **ap-name** command sets the name of an AP.

The **undo ap-name** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, no AP name is configured.

Format

ap-name *ap-new-name*

undo ap-name

Parameters

Parameter	Description	Value
ap-new-name	Specifies an AP name.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the name of an AP is changed and the change is delivered to the AP, the AP goes online using the new name.

Precautions

The new AP name cannot be the same as the existing AP name.

If the AP name is not configured, the default name of an AP is the AP's MAC address after the AP goes online.

Follow-up Procedure

Run the **commit** command to deliver the configuration to the AP.

Example

Change the AP name to **AP-N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] ap-name AP-N1-2
```

11.2.32 ap-name (AP view)

Function

The **ap-name** command configures an AP name.

The **undo ap-name** command restores the default AP name.

By default, no AP name is configured for an AP.

Format

ap-name *ap-name*

undo ap-name

Parameters

Parameter	Description	Value
ap-name	Specifies an AP name.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate AP maintenance, management, and differentiation, you can name the AP according to actual situations.

Precautions

The new AP name cannot be the same as the existing AP name.

The new AP name cannot be the same as the MAC address of an existing AP. Otherwise, the AP name will be lost after the device saves the configuration and restarts.

If a new AP name is the same as an existing AP name, the new AP is restarted after its name is changed.

If the AP name is not configured, the default name of an AP is the AP's MAC address after the AP goes online.

Example

Change the AP name to **AP-N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] ap-name AP-N1-2
```



```
Warning: The AP name of more than 31 characters does not take effect for APs in versions earlier than
V200R009C00.
Warning: This operation may cause AP reset. Continue? [Y/N]:y
```

11.2.33 ap password policy

Function

The **ap password policy** command enables the AP login password policy function and displays the AP password policy view.

The **undo ap password policy** command disables the AP login password policy function.

By default, the AP login password policy function is disabled.

Format

ap password policy

undo ap password policy

Parameters

None

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a password is configured using the **ap username** 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 a password policy for the local administrator:

- Run the **password expire** command to set the password expiration time.
- 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 historical passwords recorded for each user.

Precautions

Running the **undo ap password policy** command invalidates the password policy, posing security risks.

Example

Enable the AP login password policy function and display the AP password policy view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy]
```

11.2.34 ap-patch update load

Function

The **ap-patch update load** command loads a patch for a specified AP.

The **undo ap-patch update load** command cancels a patch upgrade from a specified AP.

Format

ap-patch update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } **update-filename** *update-file-name* [**next-startup**]

undo ap-patch update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-mac *ap-mac*	Specifies the AP's MAC address.	The specified AP's MAC address must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
update-filename *update-file-name*	Specifies the name of an AP patch file.	The value is a string of 1 to 255 case-sensitive characters. Ensure that the file name is the same as the actual patch file name, with a file name extension of .pat.
next-startup	Specifies the patch for next startup.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you load the patch for multiple APs of a specified type, a version exception will lead to a long-time patch uninstallation. In this case, before loading the patch in a batch, you can load the patch for a single AP for testing, helping detect any exception in advance and ensuring the success of subsequent batch patch loading.

If the parameter **next-startup** is specified, the patch is loaded upon next startup. If this parameter is not specified, the patch is loaded immediately and is also used for next startup.

Precautions

If the AC or AP version is earlier than V200R021C10, the patch is uninstalled when you run the **undo ap-patch update load** command to cancel the AP patch upgrade. Running this command cancels the AP patch upgrade but does not uninstall the patch only when both the AC and AP versions are V200R021C10 or later. In this case, to uninstall the patch, run the **ap-patch delete** command.

Prerequisites

In AC upgrade mode, the AP's patch file has been uploaded to the AC. In FTP or SFTP upgrade mode, the AP's patch file has been uploaded to an FTP or SFTP server.

Follow-up Procedure

Run the **display ap update status** command to check the patch loading progress.

Example

Load the patch **AirEngineX760_V200R019C10.pat** for the AP named **N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-patch update load ap-name N1-2 update-filename
AirEngineX760_V200R019C10.pat
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP
or SFTP upgrade mode is recommended. Continue? [Y/N]: y
```

11.2.35 ap-patch update multi-load

Function

The **ap-patch update multi-load** command batch loads the patch for APs.

The **undo ap-patch update multi-load** command cancels AP patch upgrades in batches.

Format

ap-patch update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] [**next-startup**]

ap-patch update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] [**next-startup**]

undo ap-patch update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

undo ap-patch update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies an AP type ID.	The AP type ID must exist.
ap-group *group-name*	Specifies an AP group.	The AP group must exist.
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
next-startup	Specifies the patch for next startup.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ap-patch update multi-load ap-type** *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] [**next-startup**] command to batch load the patch for APs by type.

- When the parameter **ap-group** *group-name* is specified, the patch is loaded only for APs of a specified type in a specified AP group.
- When the parameter **ap-name** *ap-name* or **ap-id** *ap-id* is specified, the patch is loaded only for APs of a specified type that have specified names or IDs.
- When the parameters **ap-group** *group-name*, **ap-name** *ap-name*, and **ap-id** *ap-id* are not specified, the patch is loaded for all APs of a specified type.

- When the parameter **ap-group** *group-name*, **ap-name** *ap-name*, or **ap-id** *ap-id* is different from the specified **ap-type** *type-id*, the patch is not loaded.
- If the parameter **next-startup** is specified, the patch is loaded upon next startup. If this parameter is not specified, the patch is loaded immediately and is also used for next startup.

You can run the **ap-patch update multi-load ap-group** *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] [**next-startup**] command to batch load the patch for APs by AP group.

- When the parameter **ap-name** *ap-name* or **ap-id** *ap-id* is specified, the patch is loaded only for APs in a specified group that have specified names or IDs.
- When the parameters **ap-name** *ap-name* and **ap-id** *ap-id* are not specified, the patch is loaded for all APs in a specified group.
- When the AP group to which an AP specified by **ap-name** *ap-name* or **ap-id** *ap-id* is different from the specified AP group, the patch is not loaded for the AP.
- If the parameter **next-startup** is specified, the patch is loaded upon next startup. If this parameter is not specified, the patch is loaded immediately and is also used for next startup.

Precautions

If the AC or AP version is earlier than V200R021C10, the patch is uninstalled when you run the **undo ap-patch update multi-load** command to cancel the AP patch upgrade. Running this command cancels the AP patch upgrade but does not uninstall the patch only when both the AC and AP versions are V200R021C10 or later. In this case, to uninstall the patch, run the **ap-patch delete** command.

Prerequisites

The patch file for batch loading has been configured using the **ap-patch update update-filename** command.

Follow-up Procedure

Run the **display ap update status** command to check the patch loading progress.

Example

Load the patch for all APs with the **type-id** of 56.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-patch update multi-load ap-type 56
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP or SFTP upgrade mode is recommended. Continue? [Y/N]: y
```

Load the patch for all APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-patch update multi-load ap-group group1
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP or SFTP upgrade mode is recommended. Continue? [Y/N]: y
```


11.2.36 ap-patch update update-filename

Function

The **ap-patch update update-filename** command specifies the patch file name for APs of a specified type.

The **undo ap-patch update update-filename** command cancels the patch file name configured for APs of a specified type.

Format

ap-patch update update-filename *filename* **ap-type** *type-id* [**ap-group** *ap-group-name*]

undo ap-patch update update-filename ap-type *type-id* [**ap-group** *ap-group-name*]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies an AP type ID.	The AP type ID must exist.
filename	Specifies the name of a patch file.	The value is a string of 1 to 255 case-sensitive characters. Ensure that the file name is the same as the actual patch file name, with a file name extension of .pat.
ap-group *ap-group-name*	Specifies an AP group.	The AP group must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

After **ap-group** *ap-group-name* is specified, the patch file name is configured only for APs of a specified type in this AP group.

After configuring the AP patch file name, you can batch load the patch for APs of the same type using the **ap–patch update multi-load ap-type** command.

Example

Set the patch file name of APs with the type ID of 56 to **AirEngineX760_V200R019C10.pat**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-patch update update-filename AirEngineX760_V200R019C10.pat ap-type 56
Warning: If an AP is performing the automatic upgrade, the AP will be upgraded to the latest version.
Continue?[Y/N]:y
```

11.2.37 ap-ping

Function

The **ap-ping** command uses a specified AP to ping a network device and displays the returned result.

Format

ap-ping { **ap-name** *ap-name* | **ap-id** *ap-id* } [**-c** *count* | **-s** *packetsize* | **-m** *time* | **-t** *timeout*] * *host*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of an AP used to ping other network devices.	The AP name must already exist.
ap-id *ap-id*	Specifies the ID of an AP used to ping other network devices.	The AP ID must already exist.
-c *count*	Specifies the number of ICMP Echo Request packets to be sent.	The value is an integer that ranges from 1 to 10. The default value is 4.
-s *packetsize*	Specifies the length of an Echo Request packet excluding the IP header and ICMP header.	The value is an integer that ranges from 20 to 8100, in bytes. The default value is 56 bytes.
-m *time*	Specifies the time to wait before sending the next ICMP Request packet.	The value is an integer that ranges from 1 to 5000, in milliseconds. The default value is 2000 ms.

Parameter	Description	Value
-t *timeout*	Specifies the timeout period for an ICMP Echo Response packet.	The value is an integer that ranges from 0 to 10000, in milliseconds. The default value is 2000 ms.
host	Specifies the domain name or IP address of the destination host.	The value is a string of 1 to 20 characters.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- You can run this command to check the connectivity between an AP and network device by pinging a network device from an AP.
- The prerequisite is that the AP is online and has been configured with an IP address.

Precautions

- This command may cost much time because the parameters such as waiting time affects the command running.
- Only one AP can perform the ping operation at a time.

Example

Use the AP **N1-2** to perform a ping operation.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-ping ap-name N1-2 10.1.1.1
Warning: This operation maybe takes several minutes, continue?[Y/N]:y
[HUAWEI-wlan-view]
  AP ping result
    Success count        : 4
    Failure count        : 0
    Average response time: 1 ms
    Minimum response time: 1 ms
    Maximum response time: 1 ms
```


11.2.38 ap-pki-profile (WLAN view)

Function

The **ap-pki-profile** command creates an AP PKI realm profile and enters the AP PKI realm profile view, or enters the view of an existing AP PKI realm profile.

The **undo ap-pki-profile** command deletes an AP PKI realm profile.

By default, no AP PKI realm profile is created on the device.

Format

ap-pki-profile name *profile-name*

undo ap-pki-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Indicates the name of an AP PKI realm profile.	The value is a string of 1 to 35 case-sensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").
all	Specifies all AP PKI realm profiles to be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to create an AP PKI realm profile on the AC or enter the view of an existing AP PKI realm profile to configure the AP PKI realm, facilitating unified management and maintenance of AP certificates.

Follow-up Procedure

1. Run the **pki realm (AP PKI realm profile view)** command to configure an AP PKI realm and the CA certificate, local certificate, CRL file, and private key file to be bound to the realm.
2. Run the **ap-pki-profile (AP group view and AP view)** command to bind the AP PKI realm profile to an AP or AP group.
3. Run the **load-file (WLAN view)** command to manually load a certificate file in the AP PKI realm to an AP.

Example

Create an AP PKI realm profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-pki-profile name default
[HUAWEI-wlan-ap-pki-prof-default]
```

11.2.39 ap-pki-profile (AP group view and AP view)

Function

The **ap-pki-profile** command binds an AP PKI realm profile to an AP or AP group.

The **undo ap-pki-profile** command unbinds an AP PKI realm profile from an AP or AP group.

By default, no AP PKI realm profile is bound to an AP group or AP.

Format

ap-pki-profile *profile-name*

undo ap-pki-profile

Parameters

Parameter	Description	Value
profile-name	Indicates the name of an AP PKI realm profile.	The value is a string of 1 to 35 case-sensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP PKI realm profile is created and an AP PKI realm is configured, you can run this command to bind the AP PKI realm profile to an AP or AP group.

Prerequisites

1. An AP PKI realm profile has been created using the **ap-pki-profile (WLAN view)** command.
2. An AP PKI realm and the CA certificate, local certificate, CRL file, and private key file to be bound to the realm have been configured using the **pki realm (AP PKI realm profile view)** command.

Follow-up Procedure

Run the **load-file (WLAN view)** command to manually load a certificate file in the AP PKI realm to an AP.

Example

Create an AP PKI realm profile **default** and bind it to the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-pki-profile name default
[HUAWEI-wlan-ap-pki-prof-default] quit
[HUAWEI-wlan-ap-group-group1] ap-pki-profile default
```

11.2.40 ap-regroup

Function

The **ap-regroup** command changes the group that an AP joins.

Format

ap-regroup { **ap-name** *ap-name* | **ap-id** *ap-id* } **new-group** *new-group-name*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist. The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) to separate AP IDs or use hyphens (-) to indicate continuous AP IDs. For example, **5,8,10-13,20** indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.
new-group *new-group-name*	Specifies the name of the new group to which the AP is added.	The AP group must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the current AP group is not applicable to an AP or the AP is added to an incorrect group, you can run this command to delete the AP from the current AP group and add the AP to a new AP group.

Prerequisites

The AP group has been created using the **ap-group** command.

Configuration Impact

Adding an AP to a new AP group will cause the AP to restart, interrupting services. Therefore, exercise caution when performing this operation.

Example

Change the group that an AP joins to the AP group **group1**.

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



```
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] quit
[HUAWEI-wlan-view] ap-regroup ap-name 00e0-fc76-e360 new-group group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, Whether to continue? [Y/N]:y
```

11.2.41 ap-rename

Function

The **ap-rename** command changes the name of an AP.

Format

ap-rename { **ap-name** *name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* } **new-name** *ap-new-name*

Parameters

Parameter	Description	Value
ap-name *name*	Specifies the old name of an AP.	The AP name must exist.
ap-mac *ap-mac-address*	Specifies the MAC address of an AP.	The AP's MAC address must exist.
ap-id *ap-id*	Specifies the ID of an AP.	The AP ID must exist.

Parameter	Description	Value
new-name *ap-new-name*	Specifies the new name of an AP.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

If the name of an AP conflicts with that of another or an AP requires a more proper name, you can run this command to change the name of the AP.

If a new AP name is the same as an existing AP name, the new AP is restarted after its name is changed.

Example

Change the AP name from **N1-2** to **N2-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-rename ap-name N1-2 new-name N2-2
Warning: The AP name of more than 31 characters does not take effect for APs in versions earlier than V200R009C00.
Warning: This operation may cause AP reset. Continue? [Y/N]:y
```

11.2.42 ap-reset

Function

The **ap-reset** command resets an AP.

Format

ap-reset { **all** | **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* | **ap-group** *ap-group* | **ap-type** { **type** *type-name* | **type-id** *type-id* } }

ap-reset wait-rtu-validate

Parameters

Parameter	Description	Value
all	Resets all APs.	-
ap-name *ap-name*	Resets the AP with the specified AP name.	The AP name must exist.
ap-mac *ap-mac*	Resets the AP with the specified MAC address.	The AP's MAC address must exist.
ap-id *ap-id*	Resets the AP with the specified AP ID.	The AP ID must exist. The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) to separate AP IDs or use hyphens (-) to indicate continuous AP IDs. For example, **5,8,10-13,20** indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.

Parameter	Description	Value
ap-group *ap-group*	Resets APs in the specified AP group.	The AP group must exist.
ap-type	Resets APs of the specified AP type.	-
type *type-name*	Resets APs of the specified type name.	The AP type name must exist.
type-id *type-id*	Resets APs of the specified type ID.	The AP type ID must exist.
wait-rtu-validate	Resets APs on which RTU licenses have been loaded but have not taken effect.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After in-service upgrade of APs is complete, you can run the **ap-reset** command to reset the APs. After the command is run, the APs restart with the upgraded software version. You can also use the command to restart APs for other reasons.

Prerequisites

An AP exists on the AC.

Example

Reset the AP **N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-reset ap-name N1-2
Warning: Reset AP(s), continue?[Y/N]:y
```

11.2.43 ap-system-profile (WLAN view)

Function

The **ap-system-profile** command creates an AP system profile and displays the AP system profile view, or displays the view of an existing AP system profile.

The **undo ap-system-profile** command deletes an AP system profile.

By default, the system provides the AP system profile **default**.

Format

ap-system-profile name *profile-name*

undo ap-system-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an AP system profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all AP system profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To manage and maintain multiple APs in a centralized manner, add the APs in an AP group, configure parameters in an AP system profile, and apply the AP system profile to the AP group.

To manage and maintain an AP independently, configure parameters in an AP system profile and apply the AP system profile to the AP specific profile.

Follow-up Procedure

Run the **ap-system-profile (AP group view and AP view)** command to bind the AP system profile to an AP or AP group so that the AP system profile can take effect.

Precautions

- The AP system profile **default** cannot be deleted.
- The AP system profile referenced by an AP or AP group cannot be deleted. To delete the AP system profile, unbind it from the AP or AP group first.

Example

Create the AP system profile **ap-system1** and display the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1]
```

11.2.44 ap-system-profile (AP group view and AP view)

Function

The **ap-system-profile** command binds an AP system profile to an AP or AP group.

The **undo ap-system-profile** command unbinds an AP system profile from an AP or AP group.

By default, the AP system profile **default** is bound to an AP group, but no AP system profile is bound to an AP.

Format

ap-system-profile *profile-name*

undo ap-system-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP system profile.	The AP system profile must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an AP system profile using the **ap-system-profile (WLAN view)** command, bind it to an AP or AP group so that the AP system profile can take effect.

Precautions

After an AP system profile is bound to an AP or AP group, parameter settings in the AP system profile apply to all APs using the profile.

Example

Create the AP system profile **ap-system1** and bind it to AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] ap-system-profile ap-system1
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.2.45 ap-type

Function

The **ap-type** command creates an AP type for a new AP model.

The **undo ap-type** command deletes a specified AP type.

Format

ap-type *type-description* **type-id** *type-id*

undo ap-type *type-description*

Parameters

Parameter	Description	Value
type-description	Describes an AP type.	The value is a string of 1 to 31 case-insensitive characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (" ").
type-id *type-id*	Specifies the ID of an AP type.	The value is an integer that ranges from 0 to .

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow a new AP model to connect to an AC, you can run the **ap-type** command on the AC to create an AP type for this model. If you do not need the new AP

model, you can run the **undo ap-type** command to delete the AP type of this model.

Precautions

In the **ap-type** command, ensure that the value of the *type-description* or *type-id* parameter does not conflict with the description or ID of an existing AP type. You can run the **display ap-type all** command to check existing AP types, including the default AP types that have been added during initialization and AP types that are created using commands.

Note the following points when using the **undo ap-type** command:

- The default AP types that are registered during initialization cannot be deleted.
- If configurations (for example, upgrade configurations) related to an AP type exist on the AC, this AP type cannot be deleted.

After the **ap-type** command is run to create an AP type for a new AP model, the new AP model is authorized to connect to an AC of an earlier version. However, if the connection process between the new AP model and AC is changed, the new AP model cannot connect to the AC.

Generally, you are not advised to run the **ap-type** command to create an AP type for a new model. If you want to create an AP type using this command, ensure that the mapping between *type-id* and *type-description* is configured correctly. Otherwise, the new AP model fails to connect to the AC. For the mapping between *type-id* and *type-description*, see the **AP Type Names and IDs** sheet in **Quick Reference for WLAN AP Version Mapping and Models**.

The AC does not support the type of a central AP and matching RUs running a later version.

Example

Create AP type **AP9530DN** with the ID **254** for a new AP model.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-type AP9530DN type-id 254
```

11.2.46 auto create ap-type

Function

The **auto create ap-type** command automatically imports AP types.

Format

auto create ap-type { **type-id** *type-id* | **type** *type-description* | **all** }

Parameters

Parameter	Description	Value
type-id *type-id*	Automatically imports the AP type with a specified ID.	The value is an integer that ranges from 0 to .
type *type-description*	Automatically imports the AP type with a specified description.	The value is a string of 1 to 31 characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (" ").
all	Automatically imports the types of all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

If a new AP model cannot connect to the AC, you can check whether the AP type has been created. To list the undefined AP types, run the **display ap-type undefined record** command. Then run the **auto create ap-type** command to automatically import the AP types of these APs.

The AC does not support the type of a central AP and matching RUs running a later version.

Example

Automatically import the types of all APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] auto create ap-type all
Info: 1 succeeded, 3 failed.
List of AP types that failed to be added:
--------------------------------------------------------------------------------
AP type          Type ID     Reason
--------------------------------------------------------------------------------
AP5010DN         29          This AP type already exists
AP6010DN         21          This type ID already exists
AP9910DN         133          Reached the maximum specifications of the AP type
--------------------------------------------------------------------------------
Total : 3
```


Table 11-67 Description of the **ap-type auto create ap-type** command output

Item	Description
AP type	AP type.
Type ID	ID of an AP type.
Reason	Cause of the failure to automatically import an AP type, which can be: • This AP type already exists • This type ID already exists • Reached the maximum specifications of the AP type

11.2.47 broadcast-suppression auto-detect (AP system profile view)

Function

The **broadcast-suppression auto-detect** command configures the rate limit for broadcast packets during intelligent flow control.

The **undo broadcast-suppression auto-detect** command restores the default rate limit for broadcast packets during intelligent flow control.

By default, the rate limit for broadcast packets is 256 pps.

NOTE

This function is not supported by the following models:

- AirEngine X760 series APs (excluding the AirEngine 5760-10)
- AirEngine 9700D-S (including matching ORUs)

Format

broadcast-suppression auto-detect packets *packets*

undo broadcast-suppression auto-detect

Parameters

Parameter	Description	Value
packets *packets*	Specifies the rate limit for broadcast packets.	The value is an integer that ranges from 64 to 1024, in pps.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When there are a large number of broadcast, multicast, and unknown unicast packets, the CPU becomes busy processing these packets and the buffer of the packet for receiving incoming packets is occupied. When the buffer decreases to the specified threshold, the device automatically rate-limits the broadcast, multicast, and unknown unicast packets. You can run this command to specify the rate limit for intelligent flow control as required. Rate limiting takes effect only for incoming traffic.

Example

Set the rate limit for broadcast packets during intelligent flow control to 300 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] broadcast-suppression auto-detect packets 300
```

11.2.48 capwap dtls server-auth (AP provisioning view)

Function

The **capwap dtls server-auth** { **enable** | **disable** } command enables or disables the AC authentication function for APs.

The **undo capwap dtls server-auth** command disables the device from modifying this parameter setting for APs after the configuration is delivered using the **commit** command.

By default, the AC authentication function for APs is disabled.

Format

capwap dtls server-auth { **enable** | **disable** }

undo capwap dtls server-auth

Parameters

Parameter	Description	Value
enable	Enables the AC authentication function for APs.	-

Parameter	Description	Value
disable	Disables the AC authentication function for APs.	-

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP attempts to go online, it receives Discovery Response packets from ACs and discover an available AC. A bogus AC may maliciously send a Discovery Response packet to the AP, causing the AP to go online on the bogus AC.

After the AC authentication function for APs is enabled, an AP initiates DTLS authentication to the AC before establishing a CAPWAP tunnel with it. The AP then uses the DTLS PSK or initial certificate to authenticate the AC. The CAPWAP tunnel can be established only after the authentication succeeds.

Follow-up Procedure

Run the **commit** command to deliver the configuration to APs and restart the APs to make the configuration take effect.

Precautions

This function is available only for APs running V200R022C00 or later, but does not take effect for APs running versions earlier than V200R022C00.

Example

Enable the AC authentication function for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] capwap dtls server-auth enable
```

11.2.49 capwap dtls server-auth cn (AP provisioning view)

Function

The **capwap dtls server-auth cn** command specifies the CN field used by APs to verify an AC's certificate.

The **undo capwap dtls server-auth cn** *cn-string* command clears the CN field used by APs to verify an AC's certificate.

The **undo capwap dtls server-auth cn** command disables the device from modifying this parameter setting for APs after the configuration is delivered using the **commit** command.

By default, no CN field is specified for APs to verify an AC's certificate.

Format

capwap dtls server-auth cn *cn-string*

undo capwap dtls server-auth cn *cn-string*

undo capwap dtls server-auth cn

Parameters

Parameter	Description	Value
cn-string	Verifies the CN field in certificates based on the specified character string.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the AC authentication function for APs is enabled, an AP authenticates the AC based on the initial certificate if DTLS PSK authentication is unavailable or fails for three consecutive times. In this case, you can run this command to specify the CN field used by APs to verify an AC's certificate.

After this command is run, when an AP authenticates the AC based on the initial certificate, the AP verifies the CN field of the certificate based on the specified character string. This ensures that the AP can go online only on the specified AC, thereby enhancing network security.

Prerequisites

The AC authentication function for APs has been enabled using the **capwap dtls server-auth enable** command in the AP provisioning view.

By default, the AC authentication function for APs is disabled.

Follow-up Procedure

Run the **commit** command to deliver the configuration to APs and restart the APs to make the configuration take effect.

Precautions

This configuration applies only to the scenario the AC device replacement scenarios. Note the following when configuring CN fields:

- Ensure that the configured CN field is the same as that in the initial certificate of the AC in the **default** realm, and run this command with assistance from technical support personnel. Otherwise, the AP may fail to go online. To query the CN field in the initial certificate in the **default** realm, run the **display pki certificate local realm** *default* command.
- You can run this command multiple times, and a maximum of five CN fields are supported.
- Ensure that at least two CN fields are configured and the CN field list covers all possible ACs on which APs will go online. The APs cannot go online on the AC out of the CN field list.
- If only one CN field is configured, this function does not take effect.

Example

Configure the CN fields **123.example.com** and **456.example.com** used by APs to verify an AC's.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] capwap dtls server-auth cn 123.example.com
Warning: This operation will enable the AP to verify the CN field in AC certificates using DTLS. Ensure that this field be set to the same as that in the AC certificates under the guidance of technical personnel. Otherwise, the AP cannot go online. Continue? [Y/N]:y
Warning: Ensure that at least two CNs are configured for the AP to authenticate the AC. If a multi-AC backup networking is used or the AC needs to be replaced, ensure that the CN fields in the certificates of all ACs are configured on the AP. Otherwise, the AP cannot go online. Continue? [Y/N]:y
[HUAWEI-wlan-provision-ap] capwap dtls server-auth cn 456.example.com
Warning: This operation will enable the AP to verify the CN field in AC certificates using DTLS. Ensure that this field be set to the same as that in the AC certificates under the guidance of technical personnel. Otherwise, the AP cannot go online. Continue? [Y/N]:y
Warning: Ensure that at least two CNs are configured for the AP to authenticate the AC. If a multi-AC backup networking is used or the AC needs to be replaced, ensure that the CN fields in the certificates of all ACs are configured on the AP. Otherwise, the AP cannot go online. Continue? [Y/N]:y
```

11.2.50 channel-load-mode indoor

Function

The **channel-load-mode indoor** command sets the AP channel mode to indoor mode.

The **undo channel-load-mode indoor** command restores the default channel mode of APs.

The default channel mode of an AP is outdoor mode.

Format

channel-load-mode indoor

undo channel-load-mode indoor

Parameters

None

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

In scenarios where indoor and outdoor boundaries are unclear, such as subway and train platforms, it is recommended that outdoor APs be deployed. When a large volume of data is transmitted, outdoor APs in outdoor channel mode have no sufficient channels to meet data transmission requirements. In this case, you can run the **channel-load-mode indoor** command to set the channel mode of the APs to indoor mode, so that data can be transmitted on more channels.

Precautions

This command will cause an AP running V200R019C10 or earlier to automatically restart. Therefore, exercise caution when running this command.

This function is supported only by outdoor AP models.

Example

Set the AP channel mode to indoor mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] regulatory-domain-profile name default
[HUAWEI-wlan-regulate-domain-default] channel-load-mode indoor
Warning: This operation may change the operating channels of APs and restart the APs that run
V200R019C00 or earlier. Continue? [Y/N]:y
```

11.2.51 clear configuration this

Function

The **clear configuration this** command clears all configurations in the AP provisioning view.

Format

clear configuration this

Parameters

None

Views

AP provisioning view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure new AP provisioning parameters, run the **clear configuration this** command in the AP provisioning view to clear existing configurations.

Configuration Impact

Configurations in the AP provisioning view cannot be restored after they are cleared. Therefore, exercise caution when running the **clear configuration this** command.

Example

Clear all configurations in the AP provisioning view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] clear configuration this
```

11.2.52 commit (AP provisioning view)

Function

The **commit** command commits configuration to an AP, a group of APs, or all the online APs.

Format

commit { **ap-name** *ap-name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* | **ap-group** *ap-group-name* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Commits configuration to the AP with the specified AP name.	The AP name must already exist.
ap-mac *ap-mac-address*	Commits configuration to the AP with the specified MAC address.	The AP's MAC address must already exist.
ap-id *ap-id*	Commits configuration to the AP with the specified AP ID.	The AP ID must already exist.

Parameter	Description	Value
ap-group *ap-group-name*	Commits configuration to the AP in the specified AP group.	The AP group must already exist.
all	Commits configuration to all the online APs.	-

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure AP provisioning parameters on the AC, such as the AP's management VLAN, static IP address, gateway, and AC list. After the configuration is complete, run the **commit** command, and the configuration will be delivered to the AP.

Prerequisites

APs have gone online on the AC.

Precautions

- After the configuration is committed, the AP receives the configuration and compares the configuration with its local configuration.
  - If they are consistent, the AP does not process the received configuration.
  - If they are different, the AP saves the committed configuration and automatically restarts, and the received configuration takes effect.
- If the name or static IP address of an AP is specified in the AP provisioning view, the configuration is delivered only to the AP by specifying the AP name or MAC address, but cannot be delivered to APs in the specified AP group.
- If you commit configurations to a large number of APs simultaneously, some of the APs may fail to receive the configurations. In this case, you are advised to commit the configurations again.

Example

Commit the configuration to the AP with the MAC address 00e0-fc76-e360.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] commit ap-mac 00e0-fc76-e360
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and may cause reboot of AP(s). Continue?[Y/N]:y
```


11.2.53 console ble-mode (AP system profile view)

Function

The **console ble-mode** command configures the mode of the Bluetooth serial port.

The **undo console ble-mode** command restores the default mode of the Bluetooth serial port.

The default mode of the Bluetooth serial port is dynamic.

NOTE

The following models do not support the Bluetooth serial port function:

- AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
- AirEngine 5762-10 and AirEngine 5762-10SW
- AirEngine 9700D-M and AirEngine 9700D-M1

Format

console ble-mode { **dynamic** | **persistent** | **disable** }

undo console ble-mode

Parameters

Parameter	Description	Value
dynamic	Sets the mode of the Bluetooth serial port to **dynamic**. In this mode, when a Fit AP is disconnected from an AC, the Bluetooth serial port is automatically enabled; when the link between the AP and AC is normal, the Bluetooth serial port is disabled.	-
persistent	Sets the mode of the Bluetooth serial port to persistent. The Bluetooth serial port remains enabled in this mode.	-
disable	Disables the Bluetooth serial port.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the Bluetooth serial port is enabled on an AP, STAs can be connected to the AP through Bluetooth and use the CloudCampus APP to log in to the AP through the Bluetooth serial port, facilitating fault diagnosis and debugging of the AP.

Precautions

Console port login has been enabled on the AP using the **undo console disable** command.

Upon an AP restart, the Bluetooth function is automatically enabled before the AP starts up, facilitating AP fault diagnosis and debugging. If the Bluetooth serial port has been disabled using the **console ble-mode disable** command before the AP restarts, this function will be automatically disabled after the AP starts up.

Example

Set the mode of the Bluetooth serial port to **persistent** in the AP system profile **system1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] console ble-mode persistent
Warning: Bluetooth-based console port login cannot be used together with Bluetooth-based monitoring, Bluetooth-based tag locating, and Bluetooth-based transparent data transmission, Whether to continue? [Y/N]:y
```

11.2.54 console disable

Function

The **console disable** command disables a user from logging in to the AP through a console port.

The **undo console disable** command enables a user from logging in to the AP through a console port.

By default, a user can log in to the AP through a console port.

Format

console disable

undo console disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When a user cannot telnet or stelnet to the AP, the user can log in to the AP through a console port to manage and configure the AP.

After the **console disable** command is run, unauthorized users cannot log in to the AP through the console port to perform operations.

Example

Disable a user to log in to the AP through a console port.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] console disable
```

11.2.55 coordinate

Function

The **coordinate** command sets the latitude and longitude of an AP.

The **undo coordinate** command restores the latitude and longitude of an AP to empty.

By default, no latitude or longitude is configured for an AP.

NOTE

This command is not available for the following APs:

- AirEngine 5761-10W and AirEngine 5761S-10W

Format

coordinate longitude { **e** | **w** } *longitude-value* **latitude** { **s** | **n** } *latitude-value*

undo coordinate

Parameters

Parameter	Description	Value
longitude e *longitude-value*	Specifies the east longitude value of an AP.	The value supports two formats: degrees, minutes, and seconds (DMS) and decimal degrees (DD). • The DMS format is XXX-XX-XX. XXX ranges from 0 to 180, and XX ranges from 0 to 59. • The DD format is XXX.XXXXXXXXX. XXX ranges from 0 to 180, and XXXXXXXXX is a decimal supporting a maximum of 9 digits.

Parameter	Description	Value
longitude w *longitude-value*	Specifies the west longitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XXX-XX-XX. XXX ranges from 0 to 180, and XX ranges from 0 to 59. ● The DD format is XXX.XXXXXXXXX. XXX ranges from 0 to 180, and XXXXXXXXX is a decimal supporting a maximum of 9 digits.
latitude s *latitude-value*	Specifies the south latitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XX-XX-XX. The first XX ranges from 0 to 90, and the other XXs range from 0 to 59. ● The DD format is XX.XXXXXXXXX. XX ranges from 0 to 90, and XXXXXXXXX is a decimal supporting a maximum of 9 digits.
latitude n *latitude-value*	Specifies the north latitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XX-XX-XX. The first XX ranges from 0 to 90, and the other XXs range from 0 to 59. ● The DD format is XX.XXXXXXXXX. XX ranges from 0 to 90, and XXXXXXXXX is a decimal supporting a maximum of 9 digits.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to set the longitude and latitude of an AP for easily locating it.

Example

Set the longitude and latitude of an AP to 114.3435°E and 14.3435°S, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] coordinate longitude e 114.3435 latitude s 14.3435
```


11.2.56 cpu-usage threshold

Function

The **cpu-usage threshold** command configures a CPU usage alarm threshold for APs.

The **undo cpu-usage threshold** command restores the default CPU usage alarm threshold.

By default, the CPU usage alarm threshold of APs is 90.

Format

cpu-usage threshold *threshold*

undo cpu-usage threshold

Parameters

Parameter	Description	Value
threshold	Specifies the CPU usage alarm threshold of APs.	The value is an integer that ranges from 50 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **cpu-usage threshold** command to configure the CPU usage alarm threshold in the AP system profile view. The configuration is delivered to all APs using the profile.

- When the CPU usage of an AP exceeds the alarm threshold, .
- When the CPU usage of an AP falls below the alarm threshold,

Example

Set the CPU usage alarm threshold to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] cpu-usage threshold 60
```


11.2.57 cpu-defend packet-type

Function

The **cpu-defend packet-type** command configures a rate limit for packets sent by an AP to the CPU.

The **undo cpu-defend packet-type** command restores the default rate limit for packets sent by an AP to the CPU.

By default, an AP does not limit the rates of packets sent to the CPU.

Format

cpu-defend packet-type *packet-type* **rate-limit** *rate-value* { **wired** | **wireless** }

undo cpu-defend packet-type *packet-type* **rate-limit** { **wired** | **wireless** }

Parameters

Parameter	Description	Value
packet-type	Specifies the protocol type of packets.	The value depends on the protocol types supported by the device.
rate-limit *rate-value*	Specifies the rate limit. The value of *rate-value* indicates the rate limit for protocol packets.	The value is an integer that ranges from 1 to 4294967295, in pps.
wired	Indicates wired packets.	-
wireless	Indicates wireless packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an AP receives attack packets of a certain protocol type or a large number of normal packets destined for the CPU, you can limit the rates of these packets within a small range in the AP system profile to reduce the impact on CPU processing of normal services.

Precautions

If you run the **cpu-defend packet-type** command with the same *packet-type* value multiple times, only the latest configuration takes effect.

Example

Set the protocol type to wired ARP reply packet, and set the rate limit to 1260 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] cpu-defend packet-type arp-reply rate-limit 1260 wired
```

11.2.58 crc-alarm enable

Function

The **crc-alarm enable** command enables the alarm function for CRC errors on the AP's wired interface and specifies the alarm threshold and clear alarm threshold.

The **undo crc-alarm enable** command disables the alarm function for CRC errors on the AP's wired interface and restores the alarm threshold and clear alarm threshold to the default values.

By default, the alarm function for CRC errors is disabled on the AP's wired interface. The alarm threshold for CRC errors is 50 and the clear alarm threshold is 20.

Format

crc-alarm enable [**high-threshold** *high-threshold-value* | **low-threshold** *low-threshold-value*]*

undo crc-alarm enable

Parameters

Parameter	Description	Value
high-threshold *high-threshold-value*	Specifies the alarm threshold for CRC errors on the AP's wired interface.	The value is an integer that ranges from 1 to 100. The unit is 1/10000. The value of *high-threshold-value* must be larger than the value of *low-threshold-value*.
low-threshold *low-threshold-value*	Specifies the clear alarm threshold for CRC errors on the AP's wired interface.	The value is an integer that ranges from 1 to 100.

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

When the AP detects that the number of CRC errors exceeds the configured upper alarm threshold in a specified period (the time period can be configured using the **sample-time** command, and is 30s by default), it sends an alarm message to the AC. To prevent the AP from frequently sending alarm messages or alarm clearance messages to the AC, you need to configure the lower threshold for clearing the alarm. The AP sends an alarm clearance message to the AC only when the AP detects that the number of CRC errors is lower than the configured lower threshold.

Example

Enable the alarm function for CRC errors on the AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] crc-alarm enable
```

11.2.59 dai enable (AP wired port profile view)

Function

The **dai enable** command enables dynamic ARP inspection (DAI) on an AP's wired interface.

The **undo dai enable** command disables DAI on an AP's wired interface.

By default, DAI is disabled on an AP's wired interface.

Format

dai enable

undo dai enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable DAI using this command to prevent Man in The Middle (MITM) attacks and theft on authorized user information. When a device receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN ID of the ARP packet with DHCP snooping binding entries. If the ARP packet matches a binding entry, the device allows the packet to pass through. If the ARP packet does not match any binding entry, the device discards the packet.

Prerequisites

Terminal address learning has been enabled on the AP's wired interface using the **learn-client-address enable** command.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

This command takes effect only on ARP packets transmitted on an AP's wired interface.

An AP's wired interface added to an Eth-Trunk does not support this function.

Example

Enable DAI on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] dai enable
```

11.2.60 description (AP wired port profile view)

Function

The **description** command configures the description of the AP's wired interface.

The **undo description** command restores the default description of the AP's wired interface.

By default, the AP's wired interface has no description.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of the AP's wired interface.	The value is a string of 1 to 242 case-sensitive characters with spaces.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

To manage AP interfaces conveniently, run this command to set AP interface descriptions. The description of an AP interface helps you identify the AP interface and know its functions.

Example

Change the description of the AP's wired interface to **poe-power**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] description poe-power
```

11.2.61 display ap around-ssid-list

Function

The **display ap around-ssid-list** command displays SSIDs of neighbors of a specified AP.

Format

display ap around-ssid-list { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view SSIDs of neighbors of a specified AP. Neighbors of an AP include authorized and unauthorized neighbors. Authorized neighbors are other APs managed by the same AC. APs that are managed by other ACs are unauthorized neighbors.

Example

Display SSIDs of neighbors of AP **example**.

```
<HUAWEI> display ap around-ssid-list ap-name example
In control AP(2.4G):
-------------------------------------------------
SSID
-------------------------------------------------
test1
-------------------------------------------------
Total: 1
Uncontrol AP(2.4G):
-------------------------------------------------
SSID
-------------------------------------------------
test2
-------------------------------------------------
Total: 1
In control AP(5G):
-------------------------------------------------
SSID
-------------------------------------------------
test3
-------------------------------------------------
Total: 1
Uncontrol AP(5G):
-------------------------------------------------
SSID
-------------------------------------------------
test4
-------------------------------------------------
Total: 1
```

Table 11-68 Description of the **display ap around-ssid-list** command output

Item	Description
In control AP	SSIDs of authorized neighbors.
Uncontrol AP	SSIDs of unauthorized neighbors.

11.2.62 display ap asyn-message err-info

Function

The **display ap asyn-message err-info** command displays records about AP restart failures.

Format

display ap asyn-message err-info { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Displays records about restart failures of all APs.	-
ap-name *ap-name*	Displays records about restart failures of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays records about restart failures of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you use commands on the AC to restart an AP manually, during an upgrade, or to restore its factory settings, the restart message delivered by the AC may get lost due to transmission failures. Therefore, APs are not restarted. If an AP does not receive the restart message, the AP is still connected to the AC, which makes the AC incorrectly consider that the AP is restarted successfully. This command displays records about AP restart failures, helping you check whether the AP is restarted successfully. If the AP restart fails, restart the AP.

Example

Display records about restart failures of all APs.

```
<HUAWEI> display ap asyn-message err-info all
--------------------------------------------------------------------------------
AP Name MAC           Time                Reason
--------------------------------------------------------------------------------
area_1  00e0-fc76-e360 2015-1-19 14:41:59     update
area_2  00e0-fc74-9640 2015-1-19 14:45:56     clear config
--------------------------------------------------------------------------------
Total: 2
```


Table 11-69 Description of the **display ap asyn-message err-info** command output

Item	Description
AP Name	Name of an AP.
MAC	MAC address of an AP.
Time	Time when AP restart fails.
Reason	Type of AP restart failures. • update: The AP fails to be restarted during an upgrade. • clear config: The AP fails to be restarted when restoring factory settings. • other: The AP fails to be restarted manually. • reset timeout: The AP fails to be restarted because the restart command execution times out.

11.2.63 display ap coordinate

Function

The **display ap coordinate** command displays information about longitudes and latitudes of APs.

Format

display ap coordinate { **all** | **ap-group** *ap-group-name* }

Parameters

Parameter	Description	Value
all	Displays information about longitudes and latitudes of all APs.	-
ap-group *ap-group-name*	Displays information about longitudes and latitudes of APs in the specified AP group.	The AP group must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view longitudes and latitudes of APs.

Example

Display information about longitudes and latitudes of all APs.

```
<HUAWEI> display ap coordinate all
-------------------------------------------------------------------------------------------------
ID   Name          Group     Longitude          Latitude
-------------------------------------------------------------------------------------------------
0    area_1        default   30.1111111°E       40.2222222°N
1    area_2        default   110°59′59"W        77°25'53"N
2    area_3        default   -                  -
-------------------------------------------------------------------------------------------------
Total: 3
```

Table 11-70 Description of the **display ap coordinate all** command output

Item	Description
ID	AP ID.
Name	AP name.
Group	AP group.
Longitude	Longitude of an AP. Its display varies depending on the format: • Example: 114°3′14″E in the format of degree/minute/second • Example: 114.3435°E in the format of decimal degree • Hyphen (-) if it is not configured
Latitude	Latitude of an AP. • Example: 114°3′14″S in the format of degree/minute/second • Example: 114.3435°S in the format of decimal degree • Hyphen (-) if it is not configured

11.2.64 display ap elabel

Function

The **display ap elabel** command displays electronic label information about a specified AP.

Format

display ap elabel { **ap-name** *ap-name* | **ap-id** *ap-id* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays electronic label information about the AP with the specified name.	The AP name must exist.
ap-id *ap-id*	Displays electronic label information about the AP with the specified ID.	The AP ID must exist.
all	Displays electronic label information of all APs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view electronic label information about an AP. An electronic label is also called permanent configuration data or information and is written in the storage device during AP testing or commissioning. An electronic label includes the AP name, serial number, manufacture date and manufacturer information.

Example

Display electronic label information about the AP named **example**.

```
<HUAWEI> display ap elabel ap-name example
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0



 [Board Properties]
 BoardType=AirEnginexxxx
 BarCode=210235xxxxxxxxxxxxx
 Item=0235xxxx
 Description=Assembling Components,AirEnginexxxx,AirEnginexxxx,AirEnginexxxx (11ax indoor,2+4 dual
bands,smart antenna,U
SB,BLE,PSE)
 Manufactured=2020-02-21
 VendorName=Huawei
 IssueNumber=00
```



```
CLEICode=
BOM=
```

Table 11-71 Description of the **display ap elabel** command output

Item	Description
ArchivesInfo Version	Electronic label version.
BoardType	AP type.
BarCode	Bar code of an AP.
Item	BOM code of an AP.
Description	English description of an AP.
Manufactured	Production date of an AP.
VendorName	Vendor name.
IssueNumber	Issue number of an AP.
CLEICode	CLEI code of an AP.
BOM	Sales BOM code of an AP.

Display electronic label information of all APs.

```
<HUAWEI> display ap elabel all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP elabel information:
--------------------------------------------------------------------------------
ID   MAC            Name     Type           SN                  Item
--------------------------------------------------------------------------------
1    00e0-fc76-e360 L1_001   AirEnginexxxx  210235xxxxxxxxxxxxxx -
2    00e0-fc76-e340 1        AirEnginexxxx  210235xxxxxxxxxxxxxx -
--------------------------------------------------------------------------------
Total: 2
```

Table 11-72 Description of the **display ap elabel all** command output

Item	Description
ID	AP ID.
MAC	MAC address of an AP.
Name	AP name.
Type	AP type.
SN	SN of an AP.
Item	BOM code of an AP.

11.2.65 display ap fan

Function

The **display ap fan** command displays fan information about an AP.

Format

display ap fan { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays fan information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays fan information about the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check fan information about an AP, including the fan speed, operating mode, and airflow direction.

Fan information query is supported only by the AirEngine 9700D-M, AirEngine 9700D-S, and AirEngine 9700D-M1.

Example

Display fan information about AP **0**.

```
<HUAWEI> display ap fan ap-id 0
-------------------------------------------------------------------------------
Fan   State    Speed rate   Mode   Airflow direction
-------------------------------------------------------------------------------
0     Running  40%          AUTO   Front-to-Back
1     Running  40%          AUTO   Front-to-Back
-------------------------------------------------------------------------------
```

Table 11-73 Description of the **display ap fan** command output

Item	Description
Fan	Fan ID.

Item	Description
State	Status of a fan. • Absent: The fan is not in position. • Abnormal: The fan is working abnormally. • Running: The fan is running. • Stop: The fan stops.
Speed rate	Ratio of the current fan speed to the full speed.
Mode	Operating mode of a fan. • AUTO: automatic mode • MANUAL: manual mode
Airflow direction	Airflow direction of a fan. • Front-to-Back: Air flows from the front to the rear.

11.2.66 display ap lldp neighbor

Function

The **display ap lldp neighbor** command displays LLDP neighbor information on a specified AP.

Format

display ap lldp neighbor { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**interface** *interface-type interface-number*] | **brief** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays LLDP neighbor information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays LLDP neighbor information about the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
interface *interface-type interface-number*	Displays LLDP neighbor information about a specified AP interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
brief	Displays brief LLDP neighbor information about APs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view LLDP neighbor information on a specified AP, including the number of LLDP neighbors, device ID, interface ID, system name system description, and management address of each neighbor. The LLDP neighbor information is reported by an AP to the connected AC.

If no parameter is specified, LLDP neighbor information about all AP interfaces is displayed.

Prerequisites

The AP has been enabled to report LLDP neighbor information by using the **lldp report enable** command in the AP system profile view.

Example

Display LLDP neighbor information on all APs.

```
<HUAWEI> display ap lldp neighbor brief
--------------------------------------------------------------------------------
Hostname  Neighbor device  Management address  Local intf  Neighbor intf        TTL
--------------------------------------------------------------------------------
hello     HUAWEI          10.10.10.3          GE0         GigabitEthernet0/0/16  119
--------------------------------------------------------------------------------
Total: 1
```


Table 11-74 Description of the **display ap lldp neighbor** command output

Item	Description
Hostname	AP name.
Neighbor device	System name of an AP neighbor.
Management address	Management address of an AP neighbor.
Local intf	Local interface of the AP.
Neighbor intf	Interface of an AP neighbor.
TTL	Time to live (TTL) of the AP neighbor information stored on the local AP.

Display LLDP neighbor information about GE0 of the AP named **hello**.

```
<HUAWEI> display ap lldp neighbor ap-name hello interface gigabitethernet 0
------------------------------------------------------------------------------
AP 1 Port 0 has 1 neighbor(s):

Basic port information
Neighbor index              : 1
Host Name                   : hello
Chassis ID type             : macAddress
Chassis ID                  : 00e0-fc76-e360
Port ID type                : interfaceName
Port ID                     : GigabitEthernet0/0/2
Time to live                : 120s
Port description            : GigabitEthernet0/0/2
System name                 : Quidway
System description          : S5720-56C-HI
                  Huawei Versatile Routing Platform Software
                  VRP (R) software,Version 5.110 (S5720 V200R023C00)
                  Copyright (C) 2007 Huawei Technologies Co., Ltd.
System capabilities supported: wlanAccessPoint telephone
System capabilities enabled  : wlanAccessPoint telephone
Management address type      : IPv4
Management address           : 10.10.10.5

DOT3 port information
------------------------------------------------------------------------------
OperMau                              : speed(1000Mbps)/duplex(Full)
Power port class                     : Unknown
PSE power supported                  : No
PSE power enabled                    : No
PSE pairs control ability            : No
Power pairs                          : Unknown
Port power classification            : Unknown
Power type                           : Type 2 PSE
Power source                         : Reserved
Power priority                       : High
PD requested power value             : 479.5(w)
PSE allocated power value            : 281.6(w)
PD requested power value Mode A      : 0.0(w)
PD requested power value Mode B      : 2335.4(w)
PSE allocated power value Alternative A  : 1055.8(w)
PSE allocated power value Alternative B  : 1488.9(w)
Power Class                          : Unknown
PSE power pairsx                     : Alternative A
Power typex                          : Type unknown
```



```
PD 4PID                          : No
PD Load                          : Single-signature
PSE maximum available power              : 421.6(w)
PSE Autoclass support            : Yes
Autoclass completed              : Idle
Autoclass request                : Completed
Power down                       : No

Legacy port information
--------------------------------------------------------------------------------
4-pair PoE Supported             : Yes
Spare pair Detection/Classification required: Yes
PD Spare Pair Desired State      : Disable
PSE Spare Pair Operational State     : Enable
--------------------------------------------------------------------------------
```

Table 11-75 Description of the **display ap lldp neighbor ap-name** *ap-name* **interface** *interface-type interface-number* command output

Item	Description
Neighbor index	Index of a neighbor.
Host Name	AP name.
Chassis ID type	ID subtype of a neighbor device. • chassisComponent: chassis alias • interfaceAlias: interface alias • portComponent: interface or backplane alias • macAddress: MAC address • networkAddress: network address • interfaceName: name of the interface • local: name of the local device
Chassis ID	ID of a neighbor device. • A MAC address is displayed when the neighbor device ID subtype is **macAddress**. • An IP address is displayed when the neighbor device ID subtype is **networkAddress**. • A character string is displayed when the neighbor device ID subtype is neither **macAddress** nor **networkAddress**.

Item	Description
Port ID type	ID subtype of the neighbor interface. • interfaceAlias: interface alias • portComponent: interface or backplane alias • macAddress: MAC address • networkAddress: network address • interfaceName: name of the interface • agentCircuitID: loopback interface ID of the DHCP relay • local: name of the local device
Port ID	ID of the neighbor interface. • A MAC address is displayed when the neighbor interface ID subtype is **macAddress**. • An IP address is displayed when the neighbor interface ID subtype is **networkAddress**. • A character string is displayed when the neighbor interface ID subtype is neither **macAddress** nor **networkAddress**.
Time to live	Time to live (TTL) of the AP neighbor information stored on the local AP.
Port description	Description of the neighbor interface.
System name	System name.
System description	System description of the neighbor.
System capabilities supported	Capabilities of the neighbor device. • other: other capabilities • repeater: repeater • bridge: bridge device • wlanAccessPoint: wireless access point • router: router • telephone: wireless device • docsisCableDevice: management station • stationOnly: base station

Item	Description
System capabilities enabled	Capabilities enabled on the neighbor device. ● other: other capabilities ● repeater: repeater ● bridge: bridge device ● wlanAccessPoint: wireless access point ● router: router ● telephone: wireless device ● docsisCableDevice: management station ● stationOnly: base station
Management address type	Management address type of the neighbor.
Management address	Management address of the neighbor.
OperMau	Speed and duplex status of a neighbor interface. ● The value of **speed** can be 10, 100, 1000, 2500, 5000, 10000, 40000, or **Unknown**. **Unknown** indicates that the neighbor device does not carry the interface speed. ● The value of **duplex** can be **Half**, **Full**, or **Unknown**. **Unknown** indicates that the neighbor device does not carry the duplex mode.
Power port class	PoE type: ● PSE: power-sourcing equipment. ● PD: powered device. ● Unknown: unknown PoE type.
PSE power supported	Whether the PSE power is supported. ● Yes: PSE power is supported. ● No: PSE power is not supported.
PSE power enabled	Whether the PSE power is enabled. ● Yes: enabled. ● No: disabled.
PSE pairs control ability	Whether the PSE control is supported. ● Yes: PSE control is supported. ● No: PSE control is not supported.

Item	Description
Power pairs	PoE remote power supply mode: • Signal: power supply mode of signal lines. • Spare: power supply mode of spare signal lines. • Unknown: an unknown remote power supply mode.
Port power classification	PD power control level on the interface: • Class0: indicates level 1. • Class1: indicates level 2. • Class2: indicates level 3. • Class3: indicates level 4. • Class4: indicates level 5. • Class5: indicates level 6. • Class6 indicates level 7. • Class7 indicates level 8. • Unknown: indicates an unknown control level.
Power type	PoE device type:
Power source	Power supply source. Type of the PSE: **Primary power source**, **Backup source**, **Reserved**, and **Unknown** Type of the PD: **PSE**, **Reserved**, **PSE and local**, and **Unknown**
Power priority	Power priority: • Critical: the highest priority. • High: the second highest priority. • Low: the lowest priority. • Unknown: unknown priority.
PD requested power value	Power requested by the PD.
PSE allocated power value	Power allocated by the PSE.
PD requested power value Mode A	Power requested by the PD in mode A.
PD requested power value Mode B	Power requested by the PD in mode B.
PSE allocated power value Alternative A	Power allocated by the PSE for a PD in mode A.

Item	Description
PSE allocated power value Alternative B	Power allocated by the PSE for a PD in mode B.
Power Class	Power class requested by the PD or allocated by the PSE.
PSE power pairsx	Mode in which the PSE supplies power to a PD.
Power typex	Working type of the device.
PD 4PID	Whether the PD supports all power receive types. ● No: The PD does not support all power receive modes. ● Yes: The PD supports all power receive types.
PD Load	Whether isolation between modes A and B is required for the PD. ● No: Isolation between modes A and B is not required for the PD. ● Yes: Isolation between modes A and B is required for the PD.
PSE maximum available power	Maximum output power of the PSE.
PSE Autoclass support	Whether the PSE supports Autoclass. ● No: The PSE does not support Autoclass. ● Yes: The PSE supports Autoclass.
Autoclass completed	Whether Autoclass is completed.
Autoclass request	Whether Autoclass is required for the PD.
Power down	Whether the PD requires power supply from the PSE.
4-pair PoE Supported	Whether the interface supports UPoE.
Spare pair Detection/Classification required	Whether the standby device supports the requirement for detection and classification.
PD Spare Pair Desired State	Requirement state of the standby PD.
PSE Spare Pair Operational State	Operation state of the standby PSE.

11.2.67 display ap led

Function

The **display ap led** command displays the indicator blinking status of an AP.

Format

display ap led { **ap-mac** *ap-mac* | **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-mac *ap-mac*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the indicator blinking status of an AP.

This function is not available for central APs.

Example

Display the indicator blinking status of the AP with the MAC address of 00e0-fc12-3456.

```
<HUAWEI> display ap led ap-mac 00e0-fc12-3456
Led status          : blink
Blink left time(s)  : 100
```


Table 11-76 Description of the **display ap led** command output

Item	Description
Led status	Blinking status of the indicator. • off: The indicator is off. • blink: The indicator is blinking. To configure the parameter, run the **led blink-time** command. • normal: The indicator is running properly. The running status of the AP is displayed according to the indicator description.
Blink left time(s)	Remaining time of the indicator blinking status.

11.2.68 display ap neighbor

Function

The **display ap neighbor** command displays information about neighbors of a radio, including authorized and unauthorized neighbors.

Format

display ap neighbor { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
radio *radio*	Specifies radio ID of an AP.	The radio ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

APs' neighbor information reflects the APs' locations and neighbor relationships, helping you plan the network.

If a neighboring AP is an authorized one, the system displays the RSSI of signals received from the neighboring AP as well as the path loss.

If a neighboring AP is an unauthorized one, the system displays only the RSSI of signals received from the neighboring AP.

Prerequisites

The radio calibration function has been enabled using the **calibrate enable { auto | manual | schedule time }** command.

Precautions

In auto radio calibration mode, APs continuously report and update neighboring information so that the AC can query the latest AP neighbor information. In manual or scheduled radio calibration mode, APs report neighbor information during radio calibration. Information about unauthorized neighbors ages 1 hour later, and that about authorized neighbor information ages 32 hours later. Neighbor information can be queried only before the aging time expires.

Example

Display information about neighbors of radio 0 on the AP named **hello**.

```
<HUAWEI> display ap neighbor ap-name hello radio 0
Info: This operation may take a few seconds. Please wait for a moment.done.
Radio: Radio ID of AP
CH/BW: Channel/Bandwidth
SC RSSI: Single-chain RSSI
In control AP:
--------------------------------------------------------------------------------------------------------------------------
------
AP ID  AP name         Radio  CH/BW     RSSI(dBm) SC RSSI(dBm) RSSI pathloss(dB)  RSRP(dBm)  RSRP
pathloss(dB)  Last Update Time
--------------------------------------------------------------------------------------------------------------------------
------
9      00e0-fc9d-c160  0      1/40M+    -61       -66          89               -71        94
2022-09-13/19:29:48
--------------------------------------------------------------------------------------------------------------------------
------
Total: 1

Uncontrol AP:
--------------------------------------------------------------------------------------------
Radio  BSSID         Channel  RSRP(dBm)  Last Update Time       SSID
--------------------------------------------------------------------------------------------
0      00e0-fcf2-d1e0 6       -78        2022-09-13/19:27:39     hw_manage_d1e0
--------------------------------------------------------------------------------------------
Total: 1
```

Table 11-77 Description of the **display ap neighbor** command output

Item	Description
In control AP	Authorized neighboring AP.

Item	Description
AP ID	ID of a neighboring AP.
AP name	Name of a neighboring AP.
Radio	Radio ID of a neighboring AP.
CH/BW	Working channel and bandwidth of a neighboring AP. **NOTE** The device displays only information about neighboring APs detected on the current channel.
RSSI(dBm)	Received signal strength indicator (RSSI) of a neighboring AP.
SC RSSI(dBm)	Single-chain RSSI.
RSSI pathloss(dB)	RSSI path loss.
RSRP(dBm)	Reference signal received power (RSRP) of a neighboring AP. The RSRP indicates the strength of the received reference signals.
RSRP pathloss(dB)	RSRP path loss.
Last Update Time	Last update time.
Uncontrol AP	Unauthorized neighboring AP.
Radio	Neighboring AP detected on an AP radio.
BSSID	BSSID of an unauthorized neighbor.
Channel	Channel that the unauthorized neighboring AP uses.
RSRP(dBm)	Strength of signals received from the neighboring AP.
Last Update Time	Latest time when the AP is detected.
SSID	SSID of an unauthorized neighbor.

11.2.69 display ap optical-info

Function

The **display ap optical-info** command displays optical module information.

Format

display ap optical-info { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays optical module information of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays optical module information of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view optical module information, including the optical module type, transmit optical power, and receive optical power.

Prerequisites

The AP has been online. You can run the **display ap** command to check the AP status.

The AP supports optical modules. You can run the **display ap-type** command to view the AP model.

NOTE

Optical module query is supported only by the following models:

- AirEngine X760 series APs (excluding the AirEngine 6760-51EI)
- AirEngine 6761-21, AirEngine 6761-21E, AirEngine 6761S-21, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761RS-11, AirEngine 5761-11EI
- AirEngine 5762-15HW
- AirEngine 8771-X1T
- AirEngine 9700D-S (including matching ORUs)
- AirEngine series central APs

Precautions

If a copper module is inserted into an optical interface, diagnostic information is not supported.

Example

Display optical module information about the AP named **example**.

```
<HUAWEI> display ap optical-info ap-name example
--------------------------------------------------------------------------------
Interface name:XGE0/0/0
--------------------------------------------------------------------------------
Common information:
  Transceiver Type                :1000_BASE_LX_SFP
  Connector                       :LC
  Wavelength(nm)                  :1310
  Transfer Distance(m)            :10000(9um)
  Copper link length(m)           :0
  Digital Diagnostic Monitoring   :NO
  Vendor name                     :FINISAR CORP.
  Vendor part number              :FTLF1318P2BTL-HW
  Vendor IEEE company ID          :36965
  Vendor revision level           :A
  Nominal bit rate(MBits/sec)     :1200
--------------------------------------------------------------------------------
Manufacture information:
  Vendor serial number            :PMK2K62
  Manufacturing Date              :2012-05-09
  Vendor name                     :FINISAR CORP.
--------------------------------------------------------------------------------
Diagnostic information:
  Temperature(degree C)           :49
  Temp High Threshold(degree C)   :90
  Temp Low Threshold(degree C)    :-45
  Supply voltage(0.1mV)           :33161
  Volt High Threshold(0.1mV)      :37000
  Volt Low Threshold(0.1mV)       :29000
  TX bias current(mA)             :19
  Bias High Threshold(mA)         :25430
  Bias Low Threshold(mA)          :1929
  RX power(0.1uw)                 :0
  RX Power High Threshold(0.1uw)  :5012
  RX Power Low Threshold(0.1uw)   :126
  TX power(0.1uw)                 :2886
  TX Power High Threshold(0.1uw)  :6310
  TX Power Low Threshold(0.1uw)   :708
--------------------------------------------------------------------------------
Interface name:XGE0/0/1
--------------------------------------------------------------------------------
Common information:
  Transceiver Type                :OC3_LONG_REACH_SFP
  Connector                       :LC
  Wavelength(nm)                  :1310
  Transfer Distance(m)            :40000(9um)
  Copper link length(m)           :0
  Digital Diagnostic Monitoring   :YES
  Vendor name                     :NEOPHOTONING
  Vendor part number              :PT7320-31-2W
  Vendor IEEE company ID          :0
  Vendor revision level           :1.0
  Nominal bit rate(MBits/sec)     :100
--------------------------------------------------------------------------------
Manufacture information:
  Vendor serial number            :A1008036407
  Manufacturing Date              :2008-10-09
  Vendor name                     :NEOPHOTONING
--------------------------------------------------------------------------------
Diagnostic information:
  Temperature(degree C)           :47
  Temp High Threshold(degree C)   :100
  Temp Low Threshold(degree C)    :-10
  Supply voltage(0.1mV)           :32808
  Volt High Threshold(0.1mV)      :34461
```



```
  Volt Low Threshold(0.1mV)          :30523
  TX bias current(mA)                :9
  Bias High Threshold(mA)            :24
  Bias Low Threshold(mA)             :0
  RX power(0.1uw)                    :0
  RX Power High Threshold(0.1uw)     :50477
  RX Power Low Threshold(0.1uw)      :152
  TX power(0.1uw)                    :5291
  TX Power High Threshold(0.1uw)     :3320
  TX Power Low Threshold(0.1uw)      :834
--------------------------------------------------------------------------------
Interface name:XGE0/0/2
--------------------------------------------------------------------------------
Common information:
  Transceiver Type                   :1000_BASE_LX_SFP
  Connector                          :LC
  Wavelength(nm)                     :1310
  Transfer Distance(m)               :10000(9um)
  Copper link length(m)              :0
  Digital Diagnostic Monitoring      :YES
  Vendor name                        :Hisense
  Vendor part number                 :LTD1302-BC+1
  Vendor IEEE company ID             :0
  Vendor revision level              :V1.0
  Nominal bit rate(MBits/sec)        :1300
--------------------------------------------------------------------------------
Manufacture information:
  Vendor serial number               :J2220000170
  Manufacturing Date                 :2012-09-20
  Vendor name                        :Hisense
--------------------------------------------------------------------------------
Diagnostic information:
  Temperature(degree C)              :37
  Temp High Threshold(degree C)      :78
  Temp Low Threshold(degree C)       :-5
  Supply voltage(0.1mV)              :32776
  Volt High Threshold(0.1mV)         :35650
  Volt Low Threshold(0.1mV)          :29000
  TX bias current(mA)                :9
  Bias High Threshold(mA)            :70
  Bias Low Threshold(mA)             :0
  RX power(0.1uw)                    :4267
  RX Power High Threshold(0.1uw)     :5012
  RX Power Low Threshold(0.1uw)      :79
  TX power(0.1uw)                    :2304
  TX Power High Threshold(0.1uw)     :10000
  TX Power Low Threshold(0.1uw)      :631
--------------------------------------------------------------------------------
Interface name:XGE0/0/3
--------------------------------------------------------------------------------
Common information:
  Transceiver Type                   :1000_BASE_LX_SFP
  Connector                          :LC
  Wavelength(nm)                     :1310
  Transfer Distance(m)               :10000(9um)
  Copper link length(m)              :0
  Digital Diagnostic Monitoring      :YES
  Vendor name                        :FINISAR CORP.
  Vendor part number                 :FTLF1318P2BTL-HW
  Vendor IEEE company ID             :36965
  Vendor revision level              :A
  Nominal bit rate(MBits/sec)        :1200
--------------------------------------------------------------------------------
Manufacture information:
  Vendor serial number               :PLTOL92
  Manufacturing Date                 :2012-05-09
  Vendor name                        :FINISAR CORP.
--------------------------------------------------------------------------------
Diagnostic information:
```



```
Temperature(degree C)              :38
Temp High Threshold(degree C)      :90
Temp Low Threshold(degree C)       :-45
Supply voltage(0.1mV)              :33061
Volt High Threshold(0.1mV)         :37000
Volt Low Threshold(0.1mV)          :29000
TX bias current(mA)                :19
Bias High Threshold(mA)            :52
Bias Low Threshold(mA)             :4
RX power(0.1uw)                    :1
RX Power High Threshold(0.1uw)     :5012
RX Power Low Threshold(0.1uw)      :126
TX power(0.1uw)                    :3219
TX Power High Threshold(0.1uw)     :6310
TX Power Low Threshold(0.1uw)      :708
--------------------------------------------------------------------------------
```

Table 11-78 Description of the **display ap optical-info** command output

Item	Description
Interface name	Name of the optical module.
Transceiver Type	Type of the optical module.
Connector	Interface type.
Wavelength(nm)	Optical wavelength, in nm.
Transfer Distance(m)	Transmission distance, in meters.
Copper link length(m)	Length of the copper cable, in meters.
Digital Diagnostic Monitoring	Whether diagnostic information about the optical module is monitored.
Vendor name	Name of the vendor.
Vendor part number	Product code provided by the vendor.
Vendor IEEE company ID	Version number provided by the vendor.
Vendor revision level	Product serial number provided by the vendor.
Nominal bit rate(MBits/sec)	Bit rate of the optical module, in Mbit/s.
Vendor serial number	Vendor sequence number of the optical module.
Manufacturing Date	Manufacturing date of the optical module.
Temperature(degree C)	Current temperature of the optical module, in °C.
Temp High Threshold(degree C)	The upper threshold for the temperature of the optical module, in °C.

Item	Description
Temp Low Threshold(degree C)	The lower threshold for the temperature of the optical module, in °C.
Supply voltage(0.1mV)	Current voltage of the optical module, in 0.1 mV.
Volt High Threshold(0.1mV)	The upper threshold for the voltage of the optical module, in 0.1 mV.
Volt Low Threshold(0.1mV)	The lower threshold for the voltage of the optical module, in 0.1 mV.
TX bias current(mA)	Bias current of the optical module, in mA.
Bias High Threshold(mA)	Upper threshold for the bias current of the optical module, in mA.
Bias Low Threshold(mA)	Lower threshold for the bias current of the optical module, in mA.
RX power(0.1uw)	Receive power of the optical module, in 0.1 uW.
RX Power High Threshold(0.1uw)	Upper receive power threshold for the optical module, in 0.1 uW.
RX Power Low Threshold(0.1uw)	Lower receive power threshold for the optical module, in 0.1 uW.
TX power(0.1uw)	Transmit power of the optical module, in 0.1 uW.
TX Power High Threshold(0.1uw)	Upper transmit power threshold for the optical module, in 0.1 uW.
TX Power Low Threshold(0.1uw)	Lower transmit power threshold for the optical module, in 0.1 uW.

11.2.70 display ap performance statistics

Function

The **display ap performance statistics** command displays performance statistics about an AP.

Format

display ap performance statistics { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays performance statistics about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays performance statistics about the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap performance statistics** command to view AP performance statistics to monitor AP performance.

Example

Display performance statistics about AP **huawei**.

```
<HUAWEI> display ap performance statistics ap-name huawei
--------------------------------------------------------------------------------
Memory usage(%)                 : 58
Memory average usage(%)         : 58
CPU usage(%)                    : 4
CPU average usage(%)            : 4
Available space size(KB)        : 1192
Device Temperature(degree C)    : 45
Environment Temperature(degree C) : -
CPU Temperature(degree C)       : -
NP Temperature(degree C)        : -
IRF0 Temperature(degree C)      : -
IRF1 Temperature(degree C)      : -
IRF2 Temperature(degree C)      : -
IRF3 Temperature(degree C)      : -
Online user number              : 0
Upstream traffic(wireless)(KB)  : 23 KB
Wireless port drop frames(RX)   : 0
Wireless port drop frames(TX)   : 0
Wireless port total bytes(RX)   : 0
Wireless port total bytes(TX)   : 0
Wireless port unicast frames(RX): 0
GigabitEthernet port 0
  port drop frames(RX)          : 0
  port drop frames(TX)          : 0
  port total Bytes(RX)          : 0
  port total Bytes(TX)          : 0
  port unknown frames(RX)       : 0
  port error frames(TX)         : 0
  port updown counts            : 0
  port output rate(Kbps)        : 0
  port input rate(Kbps)         : 1
GigabitEthernet port 1
```



```
port drop frames(RX)          : 0
port drop frames(TX)          : 0
port total Bytes(RX)          : 61210
port total Bytes(TX)          : 38218
port unknown frames(RX)       : 0
port error frames(TX)         : 0
port updown counts            : 0
port output rate(Kbps)        : 0
port input rate(Kbps)         : 1
------------------------------------------------------------------------------
```

Table 11-79 Description of the **display ap performance statistics** command output

Item	Description
Memory usage(%)	Memory usage (%).
Memory average usage(%)	Average memory usage (%).
CPU usage(%)	CPU usage (%).
CPU average usage(%)	Average CPU usage (%).
Available space size(KB)	Available space, in KB.
Device Temperature(degree C)	AP's device temperature (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
Environment Temperature(degree C)	AP's ambient temperature (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
CPU Temperature(degree C)	AP's CPU temperature (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
NP Temperature(degree C)	AP's NP module temperature (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
IRF*n* Temperature(degree C)	Temperature of IRF *n* (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
Online user number	Number of online users.
Upstream traffic(wireless)(KB)	Traffic volume on the wireless upstream interface in a specified period, in KB.

Item	Description
Wireless port drop frames(RX)	Number of discarded data frames received by the wireless interface.
Wireless port drop frames(TX)	Number of discarded data frames sent by the wireless interface.
Wireless port total bytes(RX)	Total number of bytes received by the wireless interface.
Wireless port total bytes(TX)	Total number of bytes sent by the wireless interface.
Wireless port unicast frames(RX)	Number of unicast data frames received by the wireless interface.
GigabitEthernet port x	ID of a wired interface.
port drop frames(RX)	Number of discarded data frames received by the wired interface.
port drop frames(TX)	Number of discarded data frames sent by the wired interface.
port total Bytes(RX)	Number of bytes received by the wired interface.
port total Bytes(TX)	Number of bytes sent by the wired interface.
port unknown frames(RX)	Number of unknown protocol packets received by the wired interface.
port error frames(TX)	Number of error data frames sent by the wired interface.
port updown counts	Number of times the wired interface alternates between Up and Down.
port output rate(Kbps)	Wired-side sending rate (kbps).
port input rate(Kbps)	Wired-side receiving rate (kbps).

NOTE

If the AP does not support this parameter, a hyphen (-) is displayed.

To clear wired-side statistics on an AP, run the **reset statistics** { **ap-name** *ap-name* | **ap-id** *ap-id* } [**ssid** *ssid*] command. Alternatively, you can run **reset statistics all** the command to clear statistics on all APs.

11.2.71 display ap provision

Function

The **display ap provision** command displays the configurations for an AP to go online.

Format

display ap provision ap-id *ap-id*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you set parameters for an AP to go online in the AP view, you can run this command to view the detailed configuration.

Example

Display configurations in the AP view.

```
<HUAWEI> display ap provision ap-id 0
-------------------------------------------------------------------------------
AP name                  : area_1
AP group                 : default
AP address mode          : static
IPv4 address             : -
IPv4 mask address        : -
IPv4 gateway address     : -
IPv4 AC list             : -
Management Vlan          : 2
DTLS server-auth         : enable
DTLS server-auth cn list : -
-------------------------------------------------------------------------------
```


Table 11-80 Description of the **display ap provision ap-id** *ap-id* command output

Item	Description
AP name	AP name. To configure this parameter, run the **ap-name (AP view)** command.
AP group	AP group to which an AP belongs. To configure this parameter, run the **ap-group (AP view)** command.
AP address mode	Mode in which an AP obtains an IP address. To configure this parameter, run the **address-mode (AP view)** command.
IPv4 address	Static IPv4 address of an AP. To configure this parameter, run the **ip-address (AP view)** command.
IPv4 mask address	Static IPv4 mask of an AP. To configure this parameter, run the **ip-address (AP view)** command.
IPv4 gateway address	IPv4 gateway address of an AP. To configure this parameter, run the **ip-address (AP view)** command.
IPv4 AC list	AC IPv4 address list for APs. To configure this parameter, run the **ac-list (AP view)** command.
Management Vlan	Management VLAN tag carried in CAPWAP packets sent from the AP's wired interface. To configure this parameter, run the **management-vlan** command.
DTLS server-auth	Whether the AC authentication function is enabled for the AP. To restore the default value, run the **undo capwap dtls server-auth (AP view)** command. To enable or disable this function, run the **capwap dtls server-auth (AP provisioning view)** command and run the **commit** command to deliver the configuration.

Item	Description
DTLS server-auth cn list	CN field used by APs to verify an AC's certificate. To restore the default value, run the **undo capwap dtls server-auth cn (AP view)** command. To configure the CN field, run the **capwap dtls server-auth cn (AP provisioning view)** command and run the **commit** command to deliver the configuration.

11.2.72 display ap pki certificate

Function

The **display ap pki certificate** command displays AP certification information.

Format

display ap pki certificate ap-id *ap-id* { **ca** | **local** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays certificate information about the AP with a specified ID.	The AP ID must exist.
ca	Displays information about the CA certificate.	-
local	Displays information about the local certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate.	The value must be an existing PKI realm name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap pki certificate** command to view information about the CA or local certificate of a specified AP.

Example

Display information about the CA certificate of AP 1 in the PKI realm **abc**.

```
<HUAWEI> display ap pki certificate ap-id 1 ca realm abc
Info: This operation may take a few seconds. Please wait for a moment...done.
--------------------------------------------------------------------------------
Serial Number: 0c:f0:1a:f3:67:21:44:9a:4a:eb:ec:63:75:5d:d7:5f
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
--------------------------------------------------------------------------------
Total: 1
```

Table 11-81 Description of the **display ap pki certificate** command output

Item	Description
Serial Number	Serial number of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.
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.

11.2.73 display ap pki status

Function

The **display ap pki status** command displays an AP PKI realm and the certificate file status in the PKI realm.

Format

display ap pki status [**ap-id** *ap-id*]

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays the AP PKI realm by specifying an AP ID and the certificate file status in the PKI realm.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap pki status** command to view the AP PKI realm and the certificate file status in the PKI realm.

Example

Display all AP PKI realms and the certificate file status in the PKI realms.

```
<HUAWEI> display ap pki status
-------------------------------------------------------
AP-ID REALM1     REALM2   REALM3    REALM4   REALM5
-------------------------------------------------------
0     default/ok test/nok  -/-      -/-      -/-
1     default/ok test/ok  web/nok   -/-      -/-
2     default/ok test/ok  -/-       -/-      -/-
3     default/ok test/ok  web/ok    8021x/ok -/-
4     -/-         -/-     -/-       -/-      -/-
```

Display a specified AP PKI realm and the detailed certificate file status in the PKI realm.

```
<HUAWEI> display ap pki status ap-id 1
apid                                    : 1
realm1                                  : default
ca file           : 1.txt            status   : exist
local file        : 2.txt            status   : exist
private key file   : 3.txt             status   : exist
CRL file          : 4.txt            status   : exist
realm2                                  : test
ca file           : 1.txt            status   : exist
local file        : 2.txt            status   : exist
private key file   : 3.txt             status   : exist
CRL file          : 4.txt            status   : exist
realm3                                  : web
ca file           : 1.txt            status   : exist
local file        :                  status   :
private key file   : 3.txt             status   : exist
CRL file          : 4.txt            status   : exist
realm4                                  :
ca file           :                  status   :
local file        :                  status   :
private key file   :                    status   :
CRL file          :                  status   :
```



```
realm5                                  :
ca file           :                 status   :
local file        :                 status   :
private key file   :                  status   :
CRL file          :                 status   :
```

Table 11-82 Description of the **display ap pki status** command output

Item	Description
AP-ID	AP ID.
REALMX	Name of a PKI realm. The value can be **ok** or **nok**. **ok** indicates that the file is loaded, and **nok** indicates that the file is not loaded.
apid	AP ID.
realmx	Name of a PKI realm.
ca file	CA certificate file.
local file	Local certificate file.
private key file	Private key file.
CRL file	CRL file.
status	Certificate loading status.

11.2.74 display ap port

Function

The **display ap port** command displays the AP port status and traffic information.

Format

display ap port { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* }

Parameters

Parameter	Description	Value
all	Displays port status and traffic information of all APs.	-
ap-name *ap-name*	Displays port status and traffic information of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays port status and traffic information of the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
ap-mac *ap-mac*	Displays port status and traffic information of the AP with a specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap port** command to check the port status and traffic information of online APs, which facilitates AP port maintenance and management.

Example

Display the port status and traffic information of all APs.

```
<HUAWEI> display ap port all
Info: Waiting for AP response.
--------------------------------------------------------------------------------------------------------------------------
-----
AP-ID Port   Trunk ID    State Mode Speed Duplex TX-Packets       Tx-ErrorPackets  TX-Rate(Kbps) RX-
Packets       RX-DropPackets   RX-Rate(Kbps)
--------------------------------------------------------------------------------------------------------------------------
-----
0     GE0    0(active)   up    root 1000  full   9178            0              0              12857          0              1
.....
--------------------------------------------------------------------------------------------------------------------------
-----
Printed: 1
```

Table 11-83 Description of the **display ap port** command output

Item	Description
AP-ID	AP ID.
Port	AP port.

Item	Description
Trunk ID	Whether the Eth-Trunk function is configured on the AC and whether the AP port is added to an Eth-Trunk. ● The field outside parentheses indicates the configuration on the AC. – 0: The AC is configured to add AP ports to Eth-Trunk 0. – -: The AC is not configured to add AP ports to an Eth-Trunk. ● The field in parentheses indicates the effective configuration on the AP. – -: The AP port does not support the Eth-Trunk function. – active: The AP port has been added to an Eth-Trunk. – inactive: The AP port is not added to an Eth-Trunk. The entire field is described as follows: ● 0(active): The AP port is added to Eth-Trunk 0, and this configuration is in effect. ● 0(inactive): The AC is configured to add AP ports to Eth-Trunk 0, but this configuration takes effect only after a restart. The current AP port is not in an Eth-Trunk. ● 0(-): The AC is configured to add AP ports to Eth-Trunk 0, but the current AP port does not support the Eth-Trunk function. ● -(-): The current AP port does not support the Eth-Trunk function, and the AC is not configured to add AP ports to an Eth-Trunk. ● -(active): The AC is configured to remove AP ports from an Eth-Trunk, but this configuration takes effect only after a restart. The current AP port is still in an Eth-Trunk. ● -(inactive): The AP port is configured to leave an Eth-Trunk, and this configuration is in effect.
State	Status of the AP port. ● down: The AP port is Down. ● up: The AP port is Up.
Mode	Working mode of the AP port. ● root ● middle ● endpoint
Speed	Speed of the AP port, in Mbit/s.

Item	Description
Duplex	Duplex mode of the AP port, which includes the half-duplex and full-duplex modes.
TX-Packets	Number of data frames sent by the AP port.
Tx-ErrorPackets	Number of error data frames sent by the AP port.
TX-Rate(Kbps)	Uplink rate of the AP port.
RX-Packets	Number of data frames received by the AP port.
RX-DropPackets	Number of discarded data frames that are received by the AP port.
RX-Rate(Kbps)	Downlink rate of the AP port.

11.2.75 display ap power-workmode

Function

The **display ap power-workmode** command displays the current power mode of APs.

Format

display ap power-workmode { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-group** *ap-group* }

Parameters

Parameter	Description	Value
all	Displays the current power mode of all APs.	-
ap-name *ap-name*	Displays the current power mode of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the current power mode of the AP with a specified ID.	The AP ID must exist.
ap-mac *ap-mac*	Displays the current power mode of the AP with a specified MAC address.	The AP's MAC address must exist.
ap-group *ap-group*	Displays the current power mode of APs in a specified AP group.	The AP group must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When an AP is supplied with DC or PoE power, the AP may work in low-power mode if the power fails to meet requirements. You can run this command to view the current power mode of the AP and verify that the current power mode can enable the AP to work with all functions.

Example

Display the current power mode of all APs.

```
<HUAWEI> display ap power-workmode all
------------------------------------------------------------------------------------------------------------------------
-----
ID     MAC             Name    Group     Power-workmode     Decided by
------------------------------------------------------------------------------------------------------------------------
-----
0      00e0-fc76-e360  ap_1    default   AT(Limited)        LLDP
------------------------------------------------------------------------------------------------------------------------
-----
Total: 1
```

Table 11-84 Description of the **display ap power-workmode** command output

Item	Description
ID	AP ID.
MAC	AP's MAC address.
Name	AP name.
Group	AP group to which an AP belongs.

Item	Description
Power-workmode	Current power mode of an AP. • The power mode of an AP can be AF, AT, BT60, or BT90, which presents 802.3af, 802.3at, 802.3bt Class 6, and 802.3bt Class 8, respectively. • The working mode of an AP can be Normal, Limited, or Insufficient. In Normal mode, functions of the AP are unrestricted. In Limited mode, functions of the AP are partially restricted. In Insufficient mode, the AP restarts due to insufficient power supply, and you are not advised to use the AP in this mode. Limited: For impact on AP services by insufficient power supply. Visit **Info-Finder**, select a product series, and view hardware specifications in the hardware center. You can check the power supply downgrade limits at different power supply levels. Insufficient: Check the power supply capability of the PSE or contact technical support personnel. If the value of **Power-workmode** is **AF(Insufficient)** and the AP restarts for 10 consecutive times within a short period, the possible cause is that the power supply of the AP is insufficient. After the AP restarts for the eleventh time, it enters the AF power mode. One hour later, the AP automatically restarts and restores the original power mode. During the waiting period, you can check whether the PSE power supply is stable and replace the PSE power supply if it is unstable.
Decided by	The current power mode of an AP is determined by: • LLDP: LLDP negotiation result • Hardware detect: hardware detection result • AP capability: its own highest capability • Configuration: **power force work-mode** command configuration

11.2.76 display ap power

Function

The **display ap power** command displays power supply information about an AP.

Format

display ap power { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays power supply information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays power supply information about the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check power supply information about an AP, including the power supply mode, rated voltage, and rated power.

Power supply information query is supported only by the AirEngine 9700D-M and AirEngine 9700D-S.

Example

Display power supply information about AP **0**.

```
<HUAWEI> display ap power ap-id 0
-------------------------------------------------------------------------------
PowerNo   Present   Mode   State    Voltage(V)   Power(W)
-------------------------------------------------------------------------------
PWR1      YES       AC     Normal   56           1000
-------------------------------------------------------------------------------
```


Table 11-85 Description of the **display ap power** command output

Item	Description
PowerNo	Number of a power module.
Present	Whether a power module is in position. • YES: The power module is in position. • NO: The power module is not in position.
Mode	Power supply mode of a power module. • DC: DC power supply • AC: AC power supply
State	Power supply status of a power module. • Normal: The power module has current output. • Abnormal: The power module has no current output.
Voltage(V)	Rated voltage of a power module (V).
Power(W)	Rated power of a power module (W).

11.2.77 display ap resource

Function

The **display ap resource** command displays the number of CAPWAP tunnel resources used by APs on a device.

Format

display ap resource slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a device.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the number of CAPWAP tunnel resources used by APs on a device.

Example

Display the number of CAPWAP tunnel resources used by APs on a device.

```
<HUAWEI> display ap resource slot 0
 Slot  0
------------------------------------------------------------------------------
 Number Used :0
 Number Free : 1024
 Number Total: 1024
------------------------------------------------------------------------------
```

Table 11-86 Description of the **display ap resource slot** *slot-id* command output

Item	Description
Number Used	Number of CAPWAP tunnel resources used by APs.
Number Free	Number of available CAPWAP tunnel resources.
Number Total	Total number of CAPWAP tunnel resources on the device.

11.2.78 display ap run-info

Function

The **display ap run-info** command displays the running status of an AP.

Format

display ap run-info { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the running status of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the running status of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays the AP running status. You can run this command to monitor an AP in real time.

Prerequisites

The AP works properly.

Example

Display the running status of the AP named **example**.

```
<HUAWEI> display ap run-info ap-name example
------------------------------------------------------------------------------
AP type                    : AirEnginexxxx
Country code               : CN
Software version           : V200R023C00
Hardware version           : Ver.A
BIOS version               : 623
BOM version                : 000
Memory size(MB)            : 256
Flash size(MB)             : 64
SD Card size(MB)           : -
Manufacture                : Huawei Technologies Co., Ltd.
Software vendor            : Huawei Technologies Co., Ltd.
Online time(ddd:hh:mm:ss)  : 6H:56M:26S
Run time(ddd:hh:mm:ss)     : 6H:59M:51S
NAT IP address             : 2.2.2.1
IP address                 : 192.168.109.252
IP mask                    : 255.255.255.0
Gateway                    : 192.168.109.1
DNS server                 : 0.0.0.0
AP mode                    : campus
USB                        : enable(2.5w)
PoE                        : disable
GigabitEthernet port 0
  Port speed(Mbps)         : 1000
  Port speed mode          : auto
  Port duplex              : full
```



```
  Port duplex mode            : auto
  Port state                  : down
  STP down recovery time(ddd:hh:mm:ss)        : -
GigabitEthernet port 1
  Port speed(Mbps)            : 1000
  Port speed mode             : auto
  Port duplex                 : full
  Port duplex mode            : auto
  Port state                  : up
  STP down recovery time(ddd:hh:mm:ss)        : -
......
Card status                   : slot usb: -
------------------------------------------------------------------------------
```

Table 11-87 Description of the **display ap run-info** command output

Item	Description
AP type	AP type.
Country code	Country code.
Software version	Software version of an AP.
Hardware version	Hardware version of an AP.
BIOS version	BIOS version of an AP.
BOM version	BOM version of an AP.
Memory size(MB)	Memory size of an AP, in MB.
Flash size(MB)	Flash memory size of an AP, in MB.
SD Card size(MB)	SD card size of an AP, in MB.
Manufacture	Manufacturer of an AP.
Software vendor	AP software manufacturer.
Online time(ddd:hh:mm:ss)	AP online duration.
Run time(ddd:hh:mm:ss)	Running duration of an AP.
NAT IP address	This item is displayed only when the AP is on the private network and the AC is on the public network in NAT scenarios. The value of this parameter is the translated public IP address of the AP.
IP address	AP IPv4 address.
IP mask	IP address mask of an AP.
Gateway	Gateway IP address of an AP.
DNS server	IP address of the DNS server.

Item	Description
AP mode	AP mode. campus: The AP is not added to a branch group.
USB	Whether USB is enabled. ● disable: This function is disabled. ● enable(2.5w): USB is enabled and works at the 2.5 W power. ● enable(5w): USB is enabled and works at the 5 W power. ● -: USB is not supported.
PoE	Status of the PoE function on the interface. ● disable: This function is disabled. ● enable: This function is enabled. ● -: PoE is not supported.
XGigabitEthernet port *number*	ID of the AP's XGigabitEthernet port. This item is displayed only for an AP with an XGigabitEthernet port.
MultiGE port *number*	ID of the AP's MultiGE port. This item is displayed only for an AP with a MultiGE port.
GigabitEthernet port *number*	ID of the AP's Ethernet interface.
Ethernet port *number*	Number of the AP's Ethernet port. This item is displayed only for an AP with an Ethernet port.
Port speed(Mbps)	Rate on the upstream Ethernet interface, in Mbit/s.
Port speed mode	Rate mode of the upstream Ethernet interface, including automatic and non-automatic negotiation modes.
Port duplex	Duplex type of the upstream Ethernet interface, including full duplex and half duplex.
Port duplex mode	Duplex mode of the upstream Ethernet interface, including automatic and non-automatic negotiation modes.

Item	Description
Port state	AP interface status. • down: indicates that the interface is disabled. • up: indicates that the interface is enabled. • admin shutdown: indicates that the interface is shut down. • stp shutdown: indicates that STP on the interface is disabled.
STP down recovery time(ddd:hh:mm:ss)	Remaining recovery time of the STP.
Card status	IoT card status. • -: indicates that the IoT card is not in position. • present: indicates that the IoT card is in position.

11.2.79 display ap service-config acl

Function

The **display ap service-config acl** command displays the ACL configuration on a specified AP.

Format

display ap service-config acl { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the ACL configuration on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the ACL configuration on the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can determine which ACLs have been delivered to the AP based on the command output, which helps locate and troubleshoot faults about user rights.

Example

Display the ACL configuration on AP **hello**.

```
<HUAWEI> display ap service-config acl ap-name hello
-------------------------------------------------------------------------------
Index          ACL number
-------------------------------------------------------------------------------
1              3000
2              3002
3              3015
4              3022
5              3030
-------------------------------------------------------------------------------
Total: 5
```

Table 11-88 Description of the **display ap service-config acl** command output

Item	Description
Index	Index.
ACL number	ACL number configured on an AP.
IPv6 ACL number	ACL6 number configured on an AP.

11.2.80 display ap traffic statistics wireless

Function

The **display ap traffic statistics wireless** command displays statistics about packets with the specified SSID on the radio of an AP.

Format

display ap traffic statistics wireless { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* [**ssid** *ssid*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
radio *radio-id*	Specifies the radio ID.	The radio ID must exist.
ssid *ssid*	Specifies the SSID that STAs associate with.	The value must be an existing SSID.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap traffic statistics wireless** command to view statistics about packets with the specified SSID on the radio of an AP.

After an AP performs self-healing, packet statistics on the AP radios are cleared.

The values of some command output items are displayed as 0 due to different function support specifications.

Example

Display statistics about packets with the SSID **cmcc** on radio 0 of the AP 0.

```
<HUAWEI> display ap traffic statistics wireless ap-id 0 radio 0 ssid cmcc
------------------------------------------------------------------------
Wireless bytes(RX)           : 14583149
Wireless error frames(RX)    : 10
Wireless frames(RX)          : 97419
Wireless unicast frames(RX)  : 16
Wireless dropped frames(RX)  : 0
Wireless bytes(TX)           : 1725974
Wireless error frames(TX)    : 6
Wireless frames(TX)          : 9704
Wireless unicast frames(TX)  : 9680
Wireless dropped frames(TX)  : 6
Wireless retransmitted frames: 32674
Current accessed STA number  : 0
------------------------------------------------------------------------
```

Table 11-89 Description of the **display ap traffic statistics wireless** { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* **ssid** *ssid* command output

Item	Description
Wireless bytes(RX)	Total number of bytes of data frames received by the radio.
Wireless error frames(RX)	Total number of received error frames.

Item	Description
Wireless frames(RX)	Total number of received frames.
Wireless unicast frames(RX)	Total number of received unicast frames.
Wireless dropped frames(RX)	Total number of received frames that are discarded.
Wireless bytes(TX)	Total number of bytes of data frames sent by the radio.
Wireless error frames(TX)	Total number of transmitted error frames.
Wireless frames(TX)	Total number of transmitted frames.
Wireless unicast frames(TX)	Total number of transmitted unicast frames.
Wireless dropped frames(TX)	Total number of transmitted frames that are discarded.
Wireless retransmitted frames	Total number of retransmitted frames.
Current accessed STA number	Number of STAs that connect to the AP normally.

Display packet statistics on radio 0 of the AP 0.

```
<HUAWEI> display ap traffic statistics wireless ap-id 0 radio 0
--------------------------------------------------------------------------
Wireless frames(RX)                          :506379
Wireless bytes(RX)                          :76567129
Wireless error frames(RX)                     :113998
Wireless physical layer error frames(RX)            :0
Wireless MIC error frames(RX)                 :0
Wireless private key and decrypt fail frames(RX)     :0
Wireless unicast frames(RX)                   :30
Wireless management frames(RX)                      :506379
Wireless data frames(RX)                    :0
Wireless frames(TX)                          :4949
Wireless bytes(TX)                          :855879
Wireless RTS successes(TX)                    :0
Wireless unicast frames(TX)                   :4587
Wireless broadcast frames(TX)                  :355
Wireless failure frames(TX)                  :3406
Wireless management frames(TX)                      :4725
Wireless data frames(TX)                    :0
Wireless noise(dBm)                         :-100
Wireless port up rate(Kbps)                   :40
Wireless port down rate(Kbps)                  :1
Wireless port PS-Poll Frames                 :0
Wireless port Association Request              :0
Wireless port Association Response             :0
Wireless port ReAssociation Request            :0
Wireless port ReAssociation Response           :0
Wireless port Disassociation Frames            :0
Wireless port Deauthentication Frames          :0
Wireless retry frames                       :515
Wireless PER(%)                             :0
```



```
Wireless PER of the last 5min(%)                    :0
Wireless port PLR(%)                              :0
Wireless port PLR of the last 5min(%)               :0
Wireless retransmitted rate(%)                    :0
Wireless retransmitted rate of the last 5min(%)     :0
Wireless channel utilization(%)                   :96
WMM AC_BE retry ratio(%)                           :0
WMM AC_BK retry ratio(%)                           :0
WMM AC_VI retry ratio(%)                          :0
WMM AC_VO retry ratio(%)                           :0
WMM AC_BE PLR(%)                                  :0
WMM AC_BK PLR(%)                                  :0
WMM AC_VI PLR(%)                                  :0
WMM AC_VO PLR(%)                                   :0
------------------------------------------------------------------------------
```

Table 11-90 Description of the **display ap traffic statistics wireless** { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* command output

Item	Description
Wireless frames(RX)	Total number of data frames and management frames received by the radio.
Wireless bytes(RX)	Total number of bytes of data frames received by the radio.
Wireless error frames(RX)	Total number of error frames received by the radio.
Wireless physical layer error frames(RX)	Number of error frames received at the physical layer of the radio.
Wireless MIC error frames(RX)	Number of frames with message integrity code (MIC) received by the radio.
Wireless private key and decrypt fail frames(RX)	Number of frames with incorrect keys received by the radio.
Wireless unicast frames(RX)	Total number of received unicast frames.
Wireless management frames(RX)	Number of management frames received by the radio.
Wireless data frames(RX)	Number of data frames received by the radio.
Wireless frames(TX)	Total number of transmitted frames.
Wireless bytes(TX)	Total number of bytes of data frames sent by the radio.
Wireless RTS successes(TX)	Number of Request to Send (RTS) frames that are successfully sent by the radio.

Item	Description
Wireless unicast frames(TX)	Total number of transmitted unicast frames.
Wireless broadcast frames(TX)	Number of broadcast frames sent by the radio.
Wireless failure frames(TX)	Number of frames that the radio fails to send.
Wireless management frames(TX)	Number of management frames sent from the radio.
Wireless data frames(TX)	Number of data frames sent from the radio.
Wireless noise(dBm)	Radio noise level, in dBm.
Wireless port up rate(Kbps)	Upstream rate of the radio, in kbit/s.
Wireless port down rate(Kbps)	Downstream rate of the radio, in kbit/s.
Wireless port PS-Poll Frames	Number of data frames sent by the STA working in power saving mode.
Wireless port Association Request	Number of Association Request frames.
Wireless port Association Response	Number of Association Response frames.
Wireless port ReAssociation Request	Number of Reassociation Request frames.
Wireless port ReAssociation Response	Number of Reassociation Response frames.
Wireless port Disassociation Frames	Number of Disassociation frames.
Wireless port Deauthentication Frames	Number of Deauthentication frames.
Wireless retry frames	Number of frames that are retransmitted by the radio.
Wireless PER(%)	Packet error rate of the radio.
Wireless PER of the last 5min(%)	Packet error rate of the radio in the previous statistical period (5 minutes).
Wireless port PLR(%)	Packet loss ratio of the radio.
Wireless port PLR of the last 5min(%)	Packet loss rate of the radio in the previous statistical period (5 minutes).
Wireless retransmitted rate(%)	Retransmission rate of the radio.

Item	Description
Wireless retransmitted rate of the last 5min(%)	Retransmission rate of the radio in the previous statistical period (5 minutes).
Wireless channel utilization(%)	Channel utilization of the radio. **NOTE** When an AP radio works in monitor mode, this parameter is displayed as **-**.
WMM AC_BE retry ratio(%)	Retransmission ratio of AC_BE packets in the WMM queue.
WMM AC_BK retry ratio(%)	Retransmission rate of AC_BK packets in the WMM queue.
WMM AC_VI retry ratio(%)	Retransmission ratio of AC_VI packets in the WMM queue.
WMM AC_VO retry ratio(%)	Retransmission ratio of AC_VO packets in the WMM queue.
WMM AC_BE PLR(%)	Packet loss rate of AC_BE packets in the WMM queue.
WMM AC_BK PLR(%)	Packet loss rate of AC_BK packets in the WMM queue.
WMM AC_VI PLR(%)	Packet loss rate of AC_VI packets in the WMM queue.
WMM AC_VO PLR(%)	Packet loss rate of AC_VO packets in the WMM queue.

11.2.81 display ap uncontrol all

Function

The **display ap uncontrol all** command displays information about all uncontrolled APs that are not managed by the local AC.

Format

display ap uncontrol all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about all uncontrolled APs. The command output includes channel of the controlled AP closest to the uncontrolled AP and the strength of signals that the controlled AP received from the uncontrolled AP.

Example

View information about all uncontrolled APs.

```
<HUAWEI> display ap uncontrol all
------------------------------------------------------------
BSSID          NEAREST-AP      CHANNEL  RSSI(dBm)   SSID
------------------------------------------------------------
00e0-fc76-e360 ap-13           149      -68         test
------------------------------------------------------------
Total: 1
```

Table 11-91 Description of the **display ap uncontrol all** command output

Item	Description
BSSID	BSSID of an uncontrolled AP.
NEAREST-AP	Name of the controlled AP that is closest to the uncontrolled AP.
CHANNEL	Channel on which the uncontrolled AP is detected. If a rogue AP is detected on multiple channels, the channel with the strongest signal strength is displayed.
RSSI(dBm)	Strength of signals that the closest controlled AP receives from the uncontrolled AP, in dBm.
SSID	SSID of an uncontrolled AP.

11.2.82 display ap update configuration

Function

The **display ap update configuration** command displays AP upgrade configuration.

Format

display ap update configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the AP upgrade configuration, including the upgrade mode, FTP server configuration, and SFTP server configuration.

Example

Display the AP upgrade configuration.

```
<HUAWEI> display ap update configuration
--------------------------------------------------------------------------------
AP update mode          : AC-mode
FTP configuration
 FTP IPv4 address       : -
 FTP IPv4 port          : 21
 FTP IPv4 username      :
 FTP IPv4 password      :
 FTP IPv4 max number    : 50
SFTP configuration
 SFTP IPV4 address      : -
 SFTP IPv4 port         : 22
 SFTP IPV4 username     :
 SFTP IPV4 password     :
 SFTP IPV4 max number   : 50
AP update schedule-task
 ap update schedule-task task-id 1 start-time 11:11 2017/1/1 stop-time 11:12 201 7/1/1 ap-type 54
AP type/AP-group update filename/patch filename
 AirEngine6760R-51      : AirEngineX760-V200R019C10.cc/-
--------------------------------------------------------------------------------
```

Table 11-92 Description of the **display ap update configuration** command output

Item	Description
AP update mode	AP upgrade mode. ● AC-mode: indicates the AC mode. ● FTP-mode: indicates the FTP mode. ● SFTP-mode: indicates the SFTP mode. To configure this parameter, run the **ap update mode** command.
FTP configuration	FTP server configuration.

Item	Description
FTP IPv4 address	IPv4 address of the FTP server. To configure this parameter, run the **ap update ftp-server** command.
FTP IPv4 port	IPv4 port number of the FTP server. To configure this parameter, run the **ap update ftp-server** command.
FTP IPv4 username	IPv4 user name for logging in to the FTP server. To configure this parameter, run the **ap update ftp-server** command.
FTP IPv4 password	IPv4 password for logging in to the FTP server. To configure this parameter, run the **ap update ftp-server** command.
FTP IPv4 max number	Maximum number of APs that can be upgraded simultaneously when an IPv4 address is used to access the FTP server. To configure this parameter, run the **ap update ftp-server** command.
SFTP configuration	SFTP server configuration.
SFTP IPv4 address	IPv4 address of the SFTP server. To configure this parameter, run the **ap update sftp-server** command.
SFTP IPv4 port	IPv4 port number of the SFTP server. To configure this parameter, run the **ap update sftp-server** command.
SFTP IPv4 username	IPv4 user name for logging in to the SFTP server. To configure this parameter, run the **ap update sftp-server** command.
SFTP IPv4 password	IPv4 password for logging in to the SFTP server. To configure this parameter, run the **ap update sftp-server** command.

Item	Description
SFTP IPv4 max number	Maximum number of APs that can be upgraded simultaneously when an IPv4 address is used to access the SFTP server. To configure this parameter, run the **ap update sftp-server** command.
AP update schedule-task	ID of a scheduled AP upgrade task. To configure this parameter, run the **ap update schedule-task** command.
AP type/AP-group update filename/ patch filename	Name of the upgrade file/name of the patch file for a specified AP type or group. To configure this parameter, run the **ap update update-filename** and **ap-patch update update-filename** commands.

11.2.83 display ap update schedule-task

Function

The **display ap update schedule-task** command displays information about scheduled AP upgrade tasks.

Format

display ap update schedule-task

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view information about scheduled AP upgrade tasks, and run the **undo ap update schedule-task** { **all** | **task-id** *task-id* } command to delete the scheduled tasks that have been completed or are not needed.

Example

Display information about scheduled AP upgrade tasks.

```
<HUAWEI> display ap update schedule-task
-------------------------------------------------------------------------------
 Task-ID  Task-State  Start-Time        Stop-Time         AP-Type  AP-Group
-------------------------------------------------------------------------------
 1        IDLE        2020/01/01 11:11  2020/01/02 11:12  125      -
-------------------------------------------------------------------------------
```

Table 11-93 Description of the **display ap update schedule-task** command output

Item	Description
Task-ID	ID of a scheduled AP upgrade task.
Task-State	Status of the scheduled AP upgrade task. ● DEAD: The start time of the task is earlier than the system time, or the task stops unexpectedly. ● DONE: The task is executed. ● IDLE: The task has not been activated. ● OVERTIME: The task times out. ● RUNNING: The task is running. ● WAITING: The task is in waiting state because the start time of the task has reached but a task is running.
Start-Time	Start time of the scheduled AP upgrade task.
Stop-Time	End time of the scheduled AP upgrade task.
AP-Type	Type of the APs to be upgraded.
AP-Group	AP group to which the APs to be upgraded belong.

11.2.84 display ap update status

Function

The **display ap update status** command displays the progress of upgrading Fit APs through the current AC.

Format

display ap update status { **all** | **downloading** | **failed** | **succeed** | **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-type** *ap-type* | **ap-group** *ap-group* | **waiting** }

Parameters

Parameter	Description	Value
all	Displays upgrade progress of all APs.	-
downloading	Displays APs that are upgrading.	-
failed	Displays APs that failed to be upgraded.	-
succeed	Displays APs that have been successfully upgraded.	-
ap-name *ap-name*	Displays upgrade progress of the AP with a specified name.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
ap-id *ap-id*	Displays upgrade progress of the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
ap-type *ap-type*	Displays upgrade progress of APs of a specified type.	The value is an integer. To view all AP types, run the **display ap-type all** command.
ap-group *ap-group*	Displays upgrade progress of APs in a specified AP group.	The value is a string of 1 to 35 characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?) or slashes (/), and cannot start or end with spaces or double quotation marks (" "). If the AP group name contains spaces, the input name must start and end with a quotation mark ("), for example, **"hello name1"**. The quotation marks at the beginning and end of the AP group name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
waiting	Displays APs waiting for an upgrade.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After APs are upgraded on the AC, you can run this command to view the AP upgrade progress or AP information by upgrade status.

Example

Display upgrade progress of all APs.

```
<HUAWEI> display ap update status all
FT  : File Type
N : Next startup
--------------------------------------------------------------------------------------------------------------------------
------
ID    Name      AP Type           AP Group AP MAC         FT       Update Version        Last Update Time
Update Status
--------------------------------------------------------------------------------------------------------------------------
------
0     hw0       AirEngine5760-22WD default  00e0-fc76-e320 FIT       V200R019C10SPC200B002
2020-05-19/10:11:04     succeed
1     hw1       AirEngine6760R-51  default  00e0-fc76-e340 FIT       -                     -                     -
2     hw2       AirEngine6760R-51E default  00e0-fc76-e360 FIT       V200R019C10SPC100B195
2020-05-18/19:15:41     downloading(progress: 80%/0%)
3     hw3       AirEngine9700D-M   default  00e0-fc76-e380 FIT       V200R019C10SPC200B002
2020-05-19/16:37:50     downloading(progress: 100%/50%)
--------------------------------------------------------------------------------------------------------------------------
------
Total: 4
```

Table 11-94 Description of the **display ap update status all** command output

Item	Description
ID	AP ID.
Name	AP name.
AP Type	AP type.
AP Group	AP group.
AP MAC	MAC address of an AP.
FT	Type of the AP upgrade file. **PATCH(N)** indicates that the patch is specified for next startup.
Update Version	Target version to which an AP is upgraded.
Last Update Time	Last end time when an AP is upgraded.
Update Status	AP upgrade status. For details about the upgrade status and its corresponding handling suggestions, see **Table 11-95**.

Table 11-95 AP upgrade status and handling suggestions

AP Upgrade Status	Description	Handling Suggestion
Waiting download	The AP is waiting for an upgrade.	No action is required.
downloading(progress: *x*%/*y*%)	*x*% indicates the download progress of the system software package, and *y*% indicates the progress of writing the system software package to the flash memory.	No action is required.
failed(AC global caching)	The upgrade failed. • When an AP is downloading system software package during an in-service upgrade, the system displays this message if the AP starts automatic upgrade which triggers a new process for downloading the software package. • When multiple RUs automatically upgrade at the same time, this message may also be displayed. **NOTE** In this situation, the actual RU upgrade result depends on that displayed in the **display ap update status all** command output.	Wait until the online upgrade is completed.
failed(alloc memory for file)	The upgrade failed because the AP failed to apply for memory resources.	Clear the memory of the AC, and ensure that the memory is sufficient for the AP upgrade.
failed(AP is updating now. Please wait.)	The AC delivers an upgrade instruction again when the AP is running an upgrade task.	The AP is upgrading. Wait until the upgrade is complete. If the status persists after 5 minutes, run the upgrade command again.

AP Upgrade Status	Description	Handling Suggestion
failed(AP type in the EFS mismatch)	The upgrade failed because the AP type in the EFS file trailer of the current AP version does not match the AP.	The upgrade file is incorrect. Replace the upgrade file.
failed(AP type mismatch with batch upgrade AP type)	The upgrade failed because the AP type is different from the batch upgrade AP type.	Upgrade the AC version. If the problem persists, contact technical support personnel.
failed(AP wait for fragmentation timeout)	The upgrade failed because the time that the AP waits for fragment data expired.	Check the network connection.
failed(block full)	The upgrade failed because the number of APs simultaneously upgraded in AC mode reaches the maximum.	The number of concurrent upgrades exceeds the maximum. Wait until the upgrade of other APs is complete.
failed(change to standby)	The upgrade failed due a revertive switchover failure.	Wait until the active/standby switchover is complete.
failed(fail to download the file)	The upgrade failed because the system software failed to be downloaded.	Check whether the network connection is normal or the system software package exists.
failed(file content error)	The upgrade failed due to incorrect system software file contents.	The upgrade file is incorrect. Replace the upgrade file.
failed(file version inconsistent)	The upgrade failed because the AP type in the EFS file trailer does not match the AP type contained in the system software package name.	The upgrade file is incorrect. Replace the upgrade file or upgrade the AC to the latest version.
failed(invalid file name)	The upgrade failed because the name of the AP version file is incorrect.	Ensure that the file name of the software package meets the specified requirement.
failed(link down)	The upgrade failed because the AP failed to communicate with the AC.	Check the network connection.

AP Upgrade Status	Description	Handling Suggestion
failed(mode changed)	The upgrade failed because the AP upgrade mode is changed during the AP automatic upgrade.	This is a normal process. Perform the upgrade again.
failed(nospace in AP memory)	The upgrade failed because the AP memory resources were insufficient.	Ensure that the AP memory can support the upgrade.
failed(not receive update result)	The upgrade failed because the AC receives no AP upgrade result.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(over max upgrade time)	The upgrade failed because the upgrade duration exceeds the maximum upgrade time allowed.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(server password is too long)	The upgrade failed because the FTP/SFTP server password is too long.	Change the password of the FTP/SFTP server to a value with a length less than the maximum.
failed(read file)	The upgrade failed because no upgrade file is available in the flash memory.	Check the upgrade file.
failed(receive file failed)	The upgrade failed because fragments failed to be received.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(retransfer over times)	The upgrade failed because the number of fragment retransmissions exceeds the threshold.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(send first file failed)	The upgrade failed because the first fragment failed to be sent.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(other reason)	The upgrade failed due to an unknown error.	Contact technical support personnel.

AP Upgrade Status	Description	Handling Suggestion
failed(upgrade timeout)	The upgrade timed out and failed.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(user canceled)	The upgrade failed because the user canceled the upgrade.	No action is required.
failed(waited for next batch)	The upgrade failed. The AP has to wait for the next upgrade.	No action is required.
failed(write flash error)	The upgrade failed because the system software package failed to be written to the flash memory.	Contact technical support personnel.
failed(file changed)	The upgrade failed because the upgrade file was modified during the automatic upgrade.	This is a normal process. Wait for the next upgrade.
failed(age time out)	The upgrade failed because the state machine aged out.	Check the network connection. If the network connection is normal, contact technical support personnel.
succeed	The upgrade succeeded.	No action is required.
succeed(auto resetting)	The upgrade succeeded and the AP is being automatically restarted.	No action is required.
succeed(need reset)	The upgrade succeeded. The AP must be restarted.	No action is required.
succeed(resetting)	The upgrade succeeded and the AP is being manually restarted.	No action is required.
succeed(no need to update)	The upgrade succeeded. There is no need to upgrade the AP.	No action is required.
succeed(need mode switch)	The upgrade succeeded. The AP mode needs to be switched.	No action is required.

AP Upgrade Status	Description	Handling Suggestion
failed(send upgrade configuration)	The upgrade failed because the upgrade configuration failed to be sent.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(send upgrade request)	The upgrade failed because the upgrade request failed to be sent.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(upgrade configuration response error)	The upgrade failed because there was an error in the AP's upgrade response.	Contact technical support personnel.
failed(process upgrade filename)	The upgrade failed because the AC failed to process the upgrade file name.	Contact technical support personnel.
failed(cannot get AP type)	The upgrade failed because the AC failed to obtain the AP type.	Contact technical support personnel.
failed(analyze the version by upgrade filename)	The upgrade failed because the device failed to analyze the version number in the file name.	Contact technical support personnel.
failed(state transition check failed for the update module)	The upgrade failed because the AC failed to check the status transition of the upgrade module.	Contact technical support personnel.
failed(flash component change)	The upgrade failed because the flash model is not supported.	Replace the device with one that supports the new flash memory model or contact technical support personnel.
failed(Backing up the system software)	The upgrade failed because the system software is being synchronized from the main area to the standby area.	Wait until the synchronization between the active and standby areas is complete.

AP Upgrade Status	Description	Handling Suggestion
failed (incompatible hardware BOM version)	The upgrade failed because the AP hardware of the target version is incompatible with the BOM version.	The AP does not support downgrade. No action is required.
failed(patch checksum error)	The upgrade failed because of a patch checksum error.	Check the integrity of the patch file.
failed(patch file error)	The upgrade failed because of a patch file error.	Check the integrity of the patch file.
failed (patch active failed)	The upgrade failed because of a failure to activate the patch.	Check whether the patch and the software package match with each other.
failed(vrp patch process active failed)	The upgrade failed because of a failure to activate the patch on the control plane.	Contact technical support personnel.
failed(vfp patch active failed)	The upgrade failed because of a failure to activate the patch on the forwarding plane.	Contact technical support personnel.
failed(kernel patch actived)	The upgrade failed because of a failure to activate the kernel patch.	Contact technical support personnel.
failed(patch inner proc error)	The upgrade failed because of an internal patch processing failure.	Contact technical support personnel.
failed(wifi target chip patch active failed)	The upgrade failed because of a failure to activate the Wi-Fi chip patch.	Contact technical support personnel.
failed(the current AP version does not support patch updates)	The upgrade failed because the AP version does not support the patch upgrade.	No action is required.
failed(insufficient space on the AP flash memory)	The upgrade failed due to insufficient space on the AP's flash memory.	Delete unnecessary files from the flash memory.

AP Upgrade Status	Description	Handling Suggestion
failed(nospace in AC memory)	The upgrade failed because the AC memory resources were insufficient.	Upgrade or restart the AP during off-peak hours.
failed(patch version mismatch)	The upgrade failed because the patch version does not match the AP version.	Check the patch version.
failed(The current AP version does not support the change of the FTP/SFTP server port.)	The upgrade failed because the FTP/SFTP port number of the AP cannot be changed.	Use the default FTP/SFTP port for the upgrade.
failed(The AP or AP version does not support the HOUP-based upgrade)	The upgrade failed because the current AP or AP version does not support the HOUP upgrade mode.	Use FTP or SFTP to perform the upgrade.
failed(The FTP server does not support the REST command)	The upgrade failed because the FTP server does not support REST commands.	Replace the FTP server.
failed(The AP version does not support the configuration for specifying the patch to take effect upon the next startup)	The upgrade failed because the current AP version does not support the configuration for specifying the patch for next startup.	When installing the patch, do not specify the parameter **next-startup** in the command.
failed(AP type not config)	The AP type is different from the AP type specified for the batch upgrade.	Perform the upgrade again or contact technical support personnel.
failed(The rate of the optical module does not match)	The upgrade failed because the rate of the optical module does not match.	The AP does not support downgrade. No action is required.
-	The AP requires no upgrade.	No action is required.

11.2.85 display ap update status partition

Function

The **display ap update status partition** command displays information about channel-based partitions.

Format

display ap update status partition { **all** | **partition-id** *partition-id* }

Parameters

Parameter	Description	Value
all	Displays information about all channel-based partitions.	-
partition-id *partition-id*	Displays information about the channel-based partition with a specified ID.	The value is an integer that ranges from 0 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ap update status partition** { **all** | **partition-id** *partition-id* } command displays information about the only that APs that need to be upgraded. The APs that need to be upgraded refer to those whose target version files have been loaded to the standby area and are waiting for reset.

Example

Display information about channel-based partition **1**.

```
<HUAWEI> display ap update status partition partition-id 1
PID : Partition ID
CH : Channel
-------------------------------------------------------------------------------------------------------------------------------
----------------
PID  CH  AP ID  Name   AP Type          AP Group   AP MAC         Update Version     Last Update Time
Update Status
-------------------------------------------------------------------------------------------------------------------------------
----------------
1    36  0      hw0    AirEngine6760R-51  default    00e0-fc76-e320  V200R019C10B035    2019/08/22 18:51
succeed(need reset)
2    100 1      hw1    AirEngine6760R-51  default    00e0-fc76-e340  V200R019C10B035    2019/08/22
18:51   succeed(need reset)
2    100 2      hw2    AirEngine6760R-51  default    00e0-fc76-e360  V200R019C10B035    2019/08/22
```



```
18:51   succeed(need reset)
255  -  4     hw4    AirEngine6760R-51  default    00e0-fc76-e3a0  V200R019C10B035    2019/08/22 18:51
succeed(need reset)
255  -  5     hw5    AirEngine6760R-51  default    00e0-fc76-e3c0  V200R019C10B035    2019/08/22 18:51
succeed(need reset)
--------------------------------------------------------------------------------------------------------------------
----------------
Total: 5
```

Table 11-96 Description of the **display ap update status partition** command output

Item	Description
PID	Channel-based partition ID. The value **255** indicates that a channel-based partition that does not work properly.
CH	Channel.
AP ID	AP ID.
Name	AP name.
AP Type	AP type.
AP Group	AP group.
AP MAC	AP's MAC address.
Update Version	Target version to which an AP is upgraded.
Last Update Time	Last end time when an AP is upgraded.
Update Status	AP upgrade status. For details about the upgrade status and its corresponding handling suggestions, see **Table 11-95**.

11.2.86 display ap username

Function

The **display ap username** command displays information about users logged in to the AP.

Format

display ap username

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap username** command to view information about users logged in to the AP.

Example

Display information about users logged in to the AP.

```
<HUAWEI> display ap username
--------------------------------------------------------------------------------
AP username: admin
AP password: ******
Password control                  : Disable
Is original password              : YES
Password set time                 : 1970-01-01 00:00:00
  Password expiration             : Disable (90 days)
  Password history                : Disable  (5)
  Password alert before expiration : 30 days
  Password alert original         : Enable
  Password expired                : NO
--------------------------------------------------------------------------------
```

Table 11-97 Description of the **display ap username** command output

Item	Description
AP username	User name for logging in to the AP. To configure this parameter, run the **ap username** command.
AP password	Password for logging in to the AP. To configure this parameter, run the **ap username** command.
Password control	Whether to enable the password policy function.
Is original password	Whether a password is the initial password.
Password set time	Password setting time
Password expiration	Password validity period.
Password history	Number of historical passwords recorded for each user.
Password alert before expiration	Number of password expiration prompt days.

Item	Description
Password alert original	Whether to enable the initial password change prompt function.
Password expired	Whether a password expires.

11.2.87 display ap version

Function

The **display ap version** command displays version information about APs.

Format

display ap version { **all** | { **ap-group** *ap-group-name* | **version-name** *version-name* } * }

Parameters

Parameter	Description	Value
all	Displays version information about all APs.	-
ap-group *ap-group-name*	Displays version information about all APs of a specified AP group.	The AP group must exist.
version-name *version-name*	Displays version information about a specified AP.	The value is string of 11 to 17 characters, in the format of **VxxxRxxxCxxx** or **VxxxRxxxCxxxSPCxxx**, for example, V200R006C00 or V200R005C10SPC200.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap version** command to check version information about APs.

Example

Display version information about all APs.

```
<HUAWEI> display ap version all
Backward compatible versions : V200R020 V200R021 V200R022
The forward compatible versions depend on the AP. For the specific versions, log in to the AP and run the
"display system-information" command.
--------------------------------------------------------------------------------
ID   Name          Group   Type              Version         PatchVersion    state
--------------------------------------------------------------------------------
0    00e0-fc76-e360 default AirEngine8760-X1-PRO  V200R023C00     -            normal
--------------------------------------------------------------------------------
Total: 1
```

Table 11-98 Description of the **display ap version** command output

Item	Description
Backward compatible versions	Backward compatible version.
The forward compatible versions depend on the AP. For the specific versions, log in to the AP and run the "display system-information" command.	The forward compatible versions depend on the AP. You can log in to the AP and run the **display system-information** command to query the forward compatible versions.
ID	ID.
Name	AP name.
Group	AP group name.
Type	AP type.
Version	AP version name.
PatchVersion	AP patch version.
state	AP state. For details, see **Table 11-5**.

Table 11-99 AP state list

AP State	Description	Possible Cause	Handling Suggestion
commit-failed (cmtfa)	WLAN service configurations fail to be delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are performed for the AP. If the link between the AP and AC is disconnected or the peer end has no response, the AP enters the commit-failed state.	Check the network connection.
committing (cmt)	WLAN service configurations are being delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are being delivered to the AP. During this process, the AP is in committing state.	This is a normal state, and no action is required.
config (cfg)	WLAN service configurations are being delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. During this process, the AP is in config state.	This is a normal state, and no action is required.
config-failed (cfgfa)	WLAN service configurations fail to be delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. If the configuration delivery fails due to various reasons (such as link disconnection), the AP enters the config-failed state.	Check the network connection.
download (dload)	An AP is in upgrade state.	When an AP is performing an upgrade, it enters the download state.	When the AP upgrade is complete, check the AP state.

AP State	Description	Possible Cause	Handling Suggestion
fault	An AP fails to go online.	An AP fails to go online, which is usually caused by the following: • The AP fails to obtain an IP address or obtains an incorrect IP address. • The network between the AP and AC is faulty. • The AP fails to be authenticated. • The number of APs on an AC has reached the maximum value. • The AP is faulty. • In dual-link cold backup or N+1 backup scenario, if the link between the active and standby ACs is established properly, an AP that goes online on the active AC is in fault state on the standby AC.	Handle the AP online failure. For details, see **An AP Fails to Go Online on the AC** in the *Troubleshooting Guide*.

AP State	Description	Possible Cause	Handling Suggestion
idle	It is the initialization state of an AP before it establishes a link with the AC for the first time.	When an AP has not established a CAPWAP link with the AC, the MAC address and SN of an AP that is added offline are different from the actual MAC address and SN of the AP, or the AC cannot manage an AP due to license resource insufficiency, the AP enters the idle state.	Perform the following operations. Check whether the AP is connected to the network. If the AP connection is normal, go to next step. Check the MAC address and SN of the AP that is added offline are different from the actual MAC address and SN of the AP. If not, perform the following operations: 1. Run the **display ap all** command to check AP information. 2. Run the **undo ap** { **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** } command to delete the AP. 3. Run the **ap-id** *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }] or **ap-mac** *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*] command to add correct AP information. If the fault persists, expand the license capacity. Note that RUs managed by the AC do not occupy

AP State	Description	Possible Cause	Handling Suggestion
			license resources of the AC.
name-conflicted (namec)	The name of an AP conflicts with that of an existing AP.	The name of an AP conflicts with the name of another AP that has been online on the same AC.	Run the **ap-rename ap-id** *ap-id* **new-name** *ap-new-name* command to change the AP name.
normal (nor)	An AP is working properly.	An AP successfully goes online on an AC.	This is a normal state, and no action is required.
standby (stdby)	An AP is in normal state on the standby AC.	In the HSB scenario, if the link between the master and backup ACs is established properly, an AP is in standby state on the backup AC and in normal state on the master AC.	This is a normal state, and no action is required.
ver-mismatch (vmiss)	The version of an AP does not match that of an AC on which the AP is about to go online.	The versions of the AP and AC do not match.	Log in to Huawei technical support website and download the release notes. Based on the version mapping, upgrade the AP or AC to the matching version. • Enterprise technical support website: **https://support.huawei.com/enterprise** • Carrier technical support website: **https://support.huawei.com**

AP State	Description	Possible Cause	Handling Suggestion
countryCode-mismatch (cmiss)	The country codes of the AP and AC do not match.	The AP's current version does not support the country code configured on the AC. The country code of the AP is locked, and the country code configured on the AC is not supported.	The AP does not support the country code. Upgrade the AP or modify the country code configuration on the AC. The country code of the AP is locked. Replace the AP or change the country code on the AC to be the same as that of the AP.
type-mismatch (tmiss)	The AP type does not match that configured on the AC.	The AP type configured on the AC did not match the actual AP type.	Change the AP type configured on the AC.
unauth	An AP is not authenticated.	The AP fails to be authenticated.	Run the **display ap unauthorized record** command to query authenticated APs. Run the **ap-confirm** command to confirm unauthenticated APs and allow them to go online.

11.2.88 display ap wired-port

Function

The **display ap wired-port** command displays AP wired interface configuration.

Format

display ap wired-port *interface-type interface-number* { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an AP's wired interface.	The interface type and number need to be selected according to the actual device.
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view configurations on an AP's wired interface.

Example

Display the GE interface configuration of the AP named **example**.

```
<HUAWEI> display ap wired-port gigabitethernet 0 ap-name example
--------------------------------------------------------------------------------
Wired port number             : 0
Wired port type               : GigabitEthernet
Wired port description        :
Wired port workmode           : endpoint
Wired port STP                : disable
Wired port user isolate       : disable
Wired port PVID VLAN          : -
Wired port VLAN tagged        : -
Wired port VLAN untagged      : -
Wired port Eth-trunk          : -
Wired port LLDP               : enable
Wired port LLDP basic TLV management address: enable
Wired port LLDP basic TLV port description  : enable
Wired port LLDP basic TLV system capability : enable
Wired port LLDP basic TLV system description: enable
Wired port LLDP basic TLV system name       : enable
Wired port CRC warn switch    : No
Wired port CRC warn high threshold : 50
Wired port CRC warn low threshold  : 20
--------------------------------------------------------------------------------
Traffic Type                  Direction  AppliedRecord
--------------------------------------------------------------------------------
traffic-filter                inbound    IPv4 ACL 3012
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```



```
Traffic Type                    Direction  RemarkType  RemarkValue  AppliedRecord
--------------------------------------------------------------------------------
traffic-remark                  outbound   802.1p      2            IPv4 ACL 3011
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

Table 11-100 Description about the **display ap wired-port gigabitethernet 0 ap-name** command output

Item	Description
Wired port number	Number of the wired interface.
Wired port type	Type of the wired interface.
Wired port description	Description of the wired interface.
Wired port workmode	Mode of the wired interface.
Wired port STP	Whether STP is enabled on the wired interface.
Wired port user isolate	Whether user isolation is enabled on the wired interface.
Wired port PVID VLAN	PVID of the wired interface.
Wired port VLAN tagged	VLAN to which the interface is added in tagged mode.
Wired port VLAN untagged	VLAN to which the interface is added in untagged mode.
Wired port Eth-trunk	Trunk ID to which the wired interface is bound.
Wired port LLDP	Whether LLDP is enabled on the wired interface.
Wired port LLDP basic TLV management address	TLV of the management IP address of the wired interface.
Wired port LLDP basic TLV port description	TLV of wired interface description.
Wired port LLDP basic TLV system capability	TLV of the wired interface capability set.
Wired port LLDP basic TLV system description	TLV of wired interface system description.
Wired port LLDP basic TLV system name	TLV of the wired interface system name.
Wired port CRC warn switch	Whether to enable the alarm function for CRC errors on the wired interface.
Wired port CRC warn high threshold	Upper alarm threshold for CRC errors on the wired interface.

Item	Description
Wired port CRC warn low threshold	Lower alarm threshold for CRC errors on the wired interface.
Traffic Type	ACL-based packet filtering and re-marking implemented by the AP wired port. • traffic-filter • traffic-remark
Direction	Incoming or outgoing packets.
AppliedRecord	IPv4/IPv6/L2 packet filtering and re-marking based on ACLs.
RemarkType	Protocol type. • dscp • dot1p
RemarkValue	Protocol type value. • dscp: 0-63 • dot1p: 0-7

Display the Eth-Trunk interface configuration of the AP named **example**.

```
<HUAWEI> display ap wired-port eth-trunk 0 ap-name example
--------------------------------------------------------------------------------
Eth-trunk ID                    : 0
Eth-trunk description           : -
Workmode                        : root
STP                             : disable
User isolate                    : disable
PVID VLAN                       : -
VLAN tagged                     : -
VLAN untagged                   : -
--------------------------------------------------------------------------------
Traffic Type                    Direction  AppliedRecord
--------------------------------------------------------------------------------
traffic-filter                  inbound    IPv4 ACL 3012
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Traffic Type                    Direction  RemarkType  RemarkValue  AppliedRecord
--------------------------------------------------------------------------------
traffic-remark                  outbound   802.1p      2            IPv4 ACL 3011
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

Table 11-101 Description about the **display ap wired-port eth-trunk 0 ap-name** command output

Item	Description
Eth-trunk ID	ID of the Eth-trunk interface.
Eth-trunk description	Description of the Eth-trunk interface.

Item	Description
Workmode	Wired interface mode of an Eth-Trunk.
STP	Whether STP is enabled on the Eth-trunk interface.
User isolate	Whether user isolation is enabled on the Eth-trunk interface.
PVID VLAN	PVID of the Eth-trunk interface.
VLAN tagged	VLAN to which the Eth-trunk interface is added in tagged mode.
VLAN untagged	VLAN to which the Eth-trunk interface is added in untagged mode.
Traffic Type	ACL-based packet filtering and re-marking implemented by the AP wired port. • traffic-filter • traffic-remark
Direction	Incoming or outgoing packets.
AppliedRecord	IPv4/IPv6/L2 packet filtering and re-marking based on ACLs.
RemarkType	Protocol type. • dscp • dot1p
RemarkValue	Protocol type value. • dscp: 0-63 • dot1p: 0-7

11.2.89 display ap-pki-profile

Function

The **display ap-pki-profile** command displays information about an AP PKI realm profile.

Format

display ap-pki-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP PKI realm profiles.	-
name *profile-name*	Displays information about a specified AP PKI realm profile.	The AP PKI realm profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about an AP PKI realm profile, including the number of times the profile is referenced, PKI realms in the profile, and certificate files in the PKI realms.

Example

Display information about all AP PKI realm profiles.

```
<HUAWEI> display ap-pki-profile all
Total: 2
------------------------------------------------------------------------------
Profile name                    Reference
------------------------------------------------------------------------------
default                         5
mytest                          2
------------------------------------------------------------------------------
```

Display detailed information about a specified AP PKI realm profile.

Table 11-102 Description of the **display ap-pki-profile** command output

Item	Description
Profile name	Name of an AP PKI realm profile.
Reference	Number of times an AP PKI realm profile is referenced.
PKI realmx name	Name of a PKI realm.
ca file format	CA certificate format.
ca file name	Name of a CA certificate file.
local file format	Format of a local certificate file.

Item	Description
local file name	Name of a local certificate file.
private key file format	Format of a private key file.
private key file name	Name of a private key file.
private key file password	Decryption password of a private key file.
CRL file	Name of a CRL file.

11.2.90 display ap-system-profile

Function

The **display ap-system-profile** command displays reference and configuration information about an AP system profile.

Format

display ap-system-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP system profiles.	-
name *profile-name*	Displays information about a specified AP system profile.	The AP system profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about an AP system profile.

Example

Display information about all AP system profiles.


```
<HUAWEI> display ap-system-profile all
-------------------------------------------------------------
Profile name                Reference
-------------------------------------------------------------
default                     1
ap-system1                  0
-------------------------------------------------------------
Total: 2
```

Table 11-103 Description of the **display ap-system-profile all** command output

Item	Description
Profile name	Name of an AP system profile.
Reference	Number of times an AP system profile is referenced.

Display information about the AP system profile **ap-system1**.

```
<HUAWEI> display ap-system-profile name ap-system1
-------------------------------------------------------------------------------
AC priority                                 : -
Protect AC IP address                       : -
Primary AC                                  : -
Backup AC                                   : -
AP management VLAN                          : -
Keep service                                : disable
Keep service allow new access               : disable
Keep service allow new access no auth       : disable
Temporary management switch                 : disable
Temporary management psk                    : ******
Card connect type                           : serial
Mesh role                                   : mesh-node
Mesh route aging time(s)                    : 15
STA access mode                             : disable
STA whitelist profile                       : -
STA blacklist profile                       : -
EAPOL start mode                            : multicast
EAPOL start transform                       : equal-bssid
EAPOL response mode                         : unicast learning
EAPOL response transform                    : equal-bssid
AP LLDP message transmission delay time(s)  : 2
AP LLDP message transmission hold multiplier  : 4
AP LLDP message transmission interval time(s)  : 30
AP LLDP restart delay time(s)               : 2
AP LLDP admin status                        : txrx
AP LLDP report interval time(s)             : 30
AP LLDP report enable                       : disable
AP device high temperature threshold (degree C): -
AP environment high temperature threshold (degree C) : -
AP CPU high temperature threshold (degree C)  : -
AP NP high temperature threshold (degree C)   : -
AP device low temperature threshold (degree C) : -
AP environment low temperature threshold (degree C)  : -
AP CPU low temperature threshold (degree C)   : -
AP NP low temperature threshold (degree C)    : -
AP CPU usage threshold(%)                   : 90
AP memory usage threshold(%)                : 80
AP disk usage threshold(%)                  : 95
Alarm restriction                           : enable
Alarm restriction period(s)                 : 60
Log server IP address                       : -
Log server Port                             : -
Log record level                            : info
```



```
Ethernet port MTU(byte)                    : 1500
Telnet                                  : disable
STelnet server                           : enable
SFTP server                              : enable
Console                                 : enable
STA ARP-ND Proxy before-assoc                 : disable
Antenna output mode                        : split
Led                                     : on
Led off time range                         : -
DHCP client option12                        : ap-name
Console ble-mode                           : dynamic
Report disassoc request                     : enable
Sample time(s)                             : 30
Dynamic blacklist aging time(s)               : 600
MPP active reselection                     : disable
AP report to                              : server
Server IP                               : 0.0.0.0
Server port                               : -
AC port                                 : -
Device aging-time(minute)                    : 3
PoE max power(mW)                          : 380000
PoE power reserved(%)                      : -
PoE power threshold(%)                     : -
PoE af inrush                             : disable
PoE high inrush                            : disable
USB                                     : disable
SSH config
  Client first time                        : disable
  User interface vty 0
    Idle timeout                           : 5min 0s
    Screen length                           : 24
    ACL inbound                             : -
    ACL outbound                            : -
    ACL ipv6 inbound                        : -
    ACL ipv6 outbound                       : -
  User interface vty 1
    Idle timeout                           : 5min 0s
    Screen length                           : 24
    ACL inbound                             : -
    ACL outbound                            : -
    ACL ipv6 inbound                        : -
    ACL ipv6 outbound                       : -
  User interface vty 2
    Idle timeout                           : 5min 0s
    Screen length                           : 24
    ACL inbound                             : -
    ACL outbound                            : -
    ACL ipv6 inbound                        : -
    ACL ipv6 outbound                       : -
  User interface vty 3
    Idle timeout                           : 5min 0s
    Screen length                           : 24
    ACL inbound                             : -
    ACL outbound                            : -
    ACL ipv6 inbound                        : -
    ACL ipv6 outbound                       : -
  User interface vty 4
    Idle timeout                           : 5min 0s
    Screen length                           : 24
    ACL inbound                             : -
    ACL outbound                            : -
    ACL ipv6 inbound                        : -
    ACL ipv6 outbound                       : -
AC protect link switch mode                   : priority
AC protect link switch packet loss echo probe time          : 20
AC protect link switch packet loss start threshold(%)       : 20
AC protect link switch packet loss gap threshold(%)         : 15
Traffic optimize broadcast suppression ARP     : enable
Traffic optimize broadcast suppression IGMP    : enable
```

```
Traffic optimize broadcast suppression ND      : enable
Traffic optimize broadcast suppression DHCP    : enable
Traffic optimize broadcast suppression DHCPv6  : enable
Traffic optimize broadcast suppression MDNS    : enable
Traffic optimize broadcast suppression other broadcast       : enable
Traffic optimize broadcast suppression other multicast       : enable
Traffic optimize broadcast suppression ARP rate limit(pps)   : 256
Traffic optimize broadcast suppression IGMP rate limit(pps)  : 256
Traffic optimize broadcast suppression ND rate limit(pps)    : 256
Traffic optimize broadcast suppression DHCP rate limit(pps)  : 256
Traffic optimize broadcast suppression DHCPv6 rate limit(pps): 256
Traffic optimize broadcast suppression MDNS rate limit(pps)  : 256
Traffic optimize broadcast suppression other broadcast rate limit(pps) : 256
Traffic optimize broadcast suppression other multicast rate limit(pps) : 256
Service-experience-analysis monitor interval(s) : 30
Wmi server profile
  Index 1                              : -
  Index 2                              : -
Broadcast suppression auto-detect packets(pps)  : 256
Multicast suppression auto-detect packets(pps)  : 256
Unicast suppression auto-detect packets(pps)    : 128
Station connectivity-detect switch              : enable
Power force work-mode                           : -
NP fast-forwarding switch                       : enable
NP CAPWAP reassembly switch                     : enable
Radio mode                                   : 3radio
Terminal identify                            : enable
S-IPFPM max user flow                           : 65535
Local management switch                         : enable
Local management IPv4 address                   : 192.168.254.254/32
Service-tunnel-profile                       : -
Distribute mode switch                          : disable
Self-healing-reset timeout(h)                   : 24
AP keep online switch                        : enable
------------------------------------------------------------------------------
```

Table 11-104 Description of the **display ap-system-profile name** *profile-name* command output

Item	Description
AC priority	AC priority. To configure this parameter, run the **priority** command.
Protect AC IP address	IP address of the standby AC. To configure this parameter, run the **protect-ac** command.
Primary AC	IP address of the primary AC. To configure this parameter, run the **primary-access** command.
Backup AC	IP address of the backup AC. To configure this parameter, run the **backup-access** command.
AP management VLAN	Management VLAN for APs To configure this parameter, run the **management-vlan** command.

Item	Description
Keep service	Whether service holding upon CAPWAP link disconnection is enabled. ● enable: This function is enabled. ● disable: This function is disabled. To configure this parameter, run the **keep-service enable** command.
Keep service allow new access	Whether new STAs using the open, WEP, or WPA/WPA2-PSK security policy are allowed to go online when an AP is offline. ● enable: This function is enabled. ● disable: This function is disabled. To configure this parameter, run the **keep-service enable allow new-access** command.
Keep service allow new access no auth	Whether the offline AP allows access of new STAs using Portal or MAC address authentication. ● enable: This function is enabled. ● disable: This function is disabled. To configure this parameter, run the **keep-service enable allow new-access no-auth** command.
Temporary management switch	Whether the offline management VAP and antenna alignment VAP are enabled for APs. ● enable: The functions are enabled. ● disable: The functions are disabled. To configure this parameter, run the **temporary-management disable (AP system profile view)** command.
Card connect type	Communication connection type between IoT cards and APs. To configure this parameter, run the **card connect-type** command.
Temporary management psk	PSK of offline management VAP and antenna alignment VAP on APs. To configure this parameter, run the **temporary-management psk** command.

Item	Description
Mesh role	Mesh role. To configure this parameter, run the **mesh-role** command.
Mesh route aging time(s)	Aging time of a Mesh route. To configure the parameter, run the **mesh-route aging-time** command.
STA access mode	STA access mode. To configure this parameter, run the **sta-access-mode** command.
STA whitelist profile	Name of a STA whitelist profile referenced by an AP system profile. To configure this parameter, run the **sta-access-mode** command.
STA blacklist profile	Name of a STA blacklist profile referenced by an AP system profile. To configure this parameter, run the **sta-access-mode** command.
EAPOL start mode	EAPoL-Start packet encapsulation mode. To configure this parameter, run the **eapol-start dest-address transform-to** command.
EAPOL start transform	EAPoL-Start packet conversion mode. To configure this parameter, run the **eapol-start dest-address transform-condition** command.
EAPOL response mode	EAPoL-Response packet encapsulation mode. To configure this parameter, run the **eapol-response dest-address transform-to** command.
EAPOL response transform	EAPoL-Response packet conversion mode. To configure this parameter, run the **eapol-response dest-address transform-condition** command.
AP LLDP message transmission delay time(s)	Delay for an AP to send LLDP packets to neighbors. To configure this parameter, run the **lldp message-transmission delay (AP system profile view)** command.

Item	Description
AP LLDP message transmission hold multiplier	Hold time multiplier of AP information on neighbors. To configure this parameter, run the **lldp message-transmission hold-multiplier (AP system profile view)** command.
AP LLDP message transmission interval time(s)	Interval at which an AP sends LLDP packets to neighbors. To configure this parameter, run the **lldp message-transmission interval (AP system profile view)** command.
AP LLDP restart delay time(s)	Delay in re-enabling LLDP. To configure this parameter, run the **lldp restart-delay** command.
AP LLDP admin status	LLDP mode on an AP. ● tx: The AP sends but does not receive LLDP packets. ● rx: The AP receives but does not send LLDP packets. ● txrx: The AP sends and receives LLDP packets. To configure this parameter, run the **lldp admin-status** command.
AP LLDP report interval time(s)	Interval at which an AP reports LLDP neighbor information to an AC. To configure this parameter, run the **lldp report-interval** command.
AP LLDP report enable	Whether an AP is enabled to report information about its LLDP neighbors. To configure this parameter, run the **lldp report enable** command.
AP device high temperature threshold (degree C)	Upper device temperature alarm threshold of an AP. To configure this parameter, run the **high-temperature threshold** command.
AP environment high temperature threshold (degree C)	Upper ambient temperature alarm threshold of an AP. To configure this parameter, run the **high-temperature threshold** command.

Item	Description
AP CPU high temperature threshold (degree C)	Upper CPU temperature alarm threshold of an AP. To configure this parameter, run the **high-temperature threshold** command.
AP NP high temperature threshold (degree C)	Upper NP module temperature alarm threshold of an AP. To configure this parameter, run the **high-temperature threshold** command.
AP device low temperature threshold (degree C)	Lower device temperature alarm threshold of an AP. To configure this parameter, run the **low-temperature threshold** command.
AP environment low temperature threshold (degree C)	Lower ambient temperature alarm threshold of an AP. To configure this parameter, run the **low-temperature threshold** command.
AP CPU low temperature threshold (degree C)	Lower CPU temperature alarm threshold of an AP. To configure this parameter, run the **low-temperature threshold** command.
AP NP low temperature threshold (degree C)	Lower NP module temperature alarm threshold of an AP. To configure this parameter, run the **low-temperature threshold** command.
AP CPU usage threshold(%)	CPU usage alarm threshold of an AP. To configure this parameter, run the **cpu-usage threshold** command.
AP memory usage threshold(%)	Memory usage alarm threshold of an AP. To configure this parameter, run the **memory-usage threshold** command.
AP disk usage threshold(%)	Disk usage alarm threshold of an AP. To configure this parameter, run the **disk-usage threshold** command.

Item	Description
Alarm restriction	Alarm suppression status of an AP. To configure this parameter, run the **alarm-restriction disable** command.
Alarm restriction period(s)	Alarm suppression period of an AP. To configure this parameter, run the **alarm-restriction period** command.
Log server IP address	IP address of the log server. To configure this parameter, run the **log-server** command.
Log server Port	Port number of the log server. To configure this parameter, run the **log-server** command.
Log record level	Level of AP logs to be backed up. To configure this parameter, run the **log-record-level** command.
Ethernet port MTU(byte)	MTU of Ethernet interfaces. To configure this parameter, run the **mtu** command.
Telnet	Whether AP Telnet login is enabled. To configure this parameter, run the **telnet enable** command.
STelnet server	Whether the STelnet server function of an AP is enabled. To configure this parameter, run the **stelnet server disable** command.
SFTP server	SFTP server status of an AP. To configure this parameter, run the **sftp server disable** command.
Console	Whether AP console port login is enabled. To configure this parameter, run the **console disable** command.
STA ARP-ND Proxy before-assoc	Whether an AP is enabled to send ARP/ND proxy packets for a STA before the STA is successfully associated. To configure this parameter, run the **sta arp-nd-proxy before-assoc** command.

Item	Description
Antenna output mode	Output mode of the AP's 2.4 GHz or 5 GHz antenna. To configure this parameter, run the **antenna-output** command.
Led	Whether AP indicators are allowed to turn on. ● on: The AP indicators are allowed to turn on. ● off: The AP indicators are forbidden to turn on. To configure this parameter, run the **led off** command.
Led off time range	Time range within which the AP indicators are forbidden to turn on. To configure this parameter, run the **led off** command.
DHCP client option12	AP information contained in Option 12 carried in DHCP messages reported by an AP. ● ap-name: AP name contained in Option 12 carried in DHCP messages reported by an AP. ● ap-type ap-mac: AP type and MAC address contained in Option 12 carried in DHCP messages reported by an AP. ● disable: The Option 12 is not carried in DHCP messages reported by an AP. To configure this parameter, run the **dhcp client option12** command.
Console ble-mode	Bluetooth-based serial port login mode. ● dynamic ● persistent ● disable: The Bluetooth-based serial port login function is disabled. To configure this parameter, run the **console ble-mode (AP system profile view)** command.

Item	Description
Report disassoc request	Whether an AP is enabled to report disassociation request packets of STAs to the AC. To configure this parameter, run the **report-disassoc-request disable** command.
Sample time(s)	AP's sampling interval. To configure this parameter, run the **sample-time** command.
Dynamic blacklist aging time(s)	Aging time of a dynamic blacklist entry. To configure this parameter, run the **dynamic-blacklist aging-time** command.
MPP active reselection	Active MPP reselection. To configure this parameter, run the **mpp-active-reselection enable** command.
AP report to	Mode in which an AP reports spectrum data. ● server: The AP reports spectrum data to a spectrum server directly. ● AC: The AP reports spectrum data to a spectrum server via the AC. To configure this parameter, run the **spectrum-analysis server** command.
Server IP	IP address of the spectrum server. To configure this parameter, run the **spectrum-analysis server** command.
Server port	Port number (UDP) of the spectrum server. To configure this parameter, run the **spectrum-analysis server** command.
AC port	Port number used by the AC to receive spectrum data (in UDP packets) from the AP. To configure this parameter, run the **spectrum-analysis server** command.

Item	Description
Device aging-time(minute)	Aging time of non-Wi-Fi device data on an AC. To set the aging time, run the **spectrum-analysis non-wifi-device aging-time** command.
PoE max power(mW)	Maximum output power of the central AP. To configure this parameter, run the **poe max-power (AP system profile view)** command.
PoE power reserved(%)	Percentage of reserved PoE power to the available PoE power on the central AP. To configure this parameter, run the **poe power-reserved (AP system profile view)** command.
PoE power threshold(%)	Alarm threshold of PoE power consumption percentage on the central AP. To configure this parameter, run the **poe power-threshold (AP system profile view)** command.
PoE af inrush	PoE standard of the central AP. To configure this parameter, run the **poe af-inrush enable (AP system profile view)** command.
PoE high inrush	Whether the central AP is enabled to allow high inrush current during power-on. To configure this parameter, run the **poe high-inrush enable (AP system profile view)** command.
Group address start	Start multicast group address. To configure this parameter, run the **igmp-snooping group-bandwidth (AP system profile view)** command.
Group address end	End multicast group address. To configure this parameter, run the **igmp-snooping group-bandwidth (AP system profile view)** command.

Item	Description
Bandwidth(kbps)	Bandwidth of global multicast groups on an AP. To configure this parameter, run the **igmp-snooping group-bandwidth (AP system profile view)** command.
USB	Whether USB is enabled. To configure this parameter, run the **usb enable (AP system profile view)** command.
SSH config	SSH configurations.
Client first time	Whether initial authentication is enabled on the SSH client. To configure this parameter, run the **ssh client first-time enable (AP system profile view)** command.
User interface vty X	VTY user interface *X*. The value of *X* is an integer that ranges from 0 to 4.
Idle timeout	Timeout period of user connections. To configure this parameter, run the **user-interface vty idle-timeout** command.
Screen length	Number of lines on each terminal screen. To configure this parameter, run the **user-interface vty screen-length** command.
ACL inbound	ACL that restricts STAs with a specified IPv4 address or within a specified IPv4 address segment from logging in to the device. To configure this parameter, run the **user-interface vty acl** command.
ACL outbound	ACL that restricts IPv4 STAs who have logged in to the device from logging in to other devices. To configure this parameter, run the **user-interface vty acl** command.

Item	Description
ACL ipv6 inbound	ACL that restricts STAs with a specified IPv6 address or within a specified IPv6 address segment from logging in to the device. To configure this parameter, run the **user-interface vty acl** command.
ACL ipv6 outbound	ACL that restricts IPv6 STAs who have logged in to the device from logging in to other devices. To configure this parameter, run the **user-interface vty acl** command.
AC protect link switch mode	Active/standby link switchover mode. To configure this parameter, run the **ac protect link-switch mode** command.
AC protect link switch packet loss echo probe time	Number of Echo probe packets sent within a statistics collection interval. To configure this parameter, run the **ac protect link-switch packet-loss echo-probe-time** command.
AC protect link switch packet loss start threshold(%)	Packet loss rate start threshold for an active/standby link switchover. To configure this parameter, run the **ac protect link-switch packet-loss** command.
AC protect link switch packet loss gap threshold(%)	Packet loss rate difference threshold for an active/standby link switchover. To configure this parameter, run the **ac protect link-switch packet-loss** command.
Traffic optimize broadcast suppression ARP	Whether the suppression function is enabled for ARP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression IGMP	Whether the suppression function is enabled for IGMP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.

Item	Description
Traffic optimize broadcast suppression ND	Whether the suppression function is enabled for ND packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression DHCP	Whether the suppression function is enabled for DHCP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression DHCPv6	Whether the suppression function is enabled for DHCPv6 packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression MDNS	Whether the suppression function is enabled for mDNS packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression other broadcast	Whether the suppression function is enabled for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression other multicast	Whether the suppression function is enabled for multicast packets other than IGMP and mDNS packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression ARP rate limit(pps)	Rate limit threshold for ARP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.

Item	Description
Traffic optimize broadcast suppression IGMP rate limit(pps)	Rate limit threshold for IGMP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression ND rate limit(pps)	Rate limit threshold for ND packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression DHCP rate limit(pps)	Rate limit threshold for DHCP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression DHCPv6 rate limit(pps)	Rate limit threshold for DHCPv6 packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression MDNS rate limit(pps)	Rate limit threshold for mDNS packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression other broadcast rate limit(pps)	Rate limit threshold for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression other multicast rate limit(pps)	Rate limit threshold for multicast packets other than IGMP and mDNS packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.

Item	Description
Service-experience-analysis monitor interval(s)	Sampling interval for SEA-based application monitoring. To configure this parameter, run the **service-experience-analysis monitor interval** command.
Wmi server profile	WMI profile bound to the AP system profile. • Index 1: WMI profile with index 1 • Index 2: WMI profile with index 2 To configure this parameter, run the **wmi-server (AP system profile view)** command.
Broadcast suppression auto-detect packets(pps)	Rate limit threshold of broadcast packets. To configure this parameter, run the **broadcast-suppression auto-detect (AP system profile view)** command.
Multicast suppression auto-detect packets(pps)	Rate limit threshold of multicast packets. To configure this parameter, run the **multicast-suppression auto-detect (AP system profile view)** command.
Unicast suppression auto-detect packets(pps)	Rate limit threshold of unknown unicast packets. To configure this parameter, run the **unicast-suppression auto-detect (AP system profile view)** command.
Station connectivity-detect switch	Whether STA connectivity check is enabled. To configure this parameter, run the **station connectivity-detect disable** command.
Power force work-mode	Power supply mode of an AP. To configure this parameter, run the **power force work-mode** command.
NP fast-forwarding switch	Whether the NP fast forwarding function is enabled. To configure this parameter, run the **np fast-forwarding disable (AP system profile view)** command.

Item	Description
NP CAPWAP reassembly switch	Whether the NP CAPWAP reassembly function is enabled. To configure this parameter, run the **np capwap-reassembly (AP system profile view)** command.
Radio mode	Radio mode of an AP. To configure this parameter, run the **radio-mode** command.
CPU defend Packet type Rate limit Type	Rate limit for packets sent by an AP to the CPU. To configure these parameters, run the **cpu-defend packet-type** command. If this command is not configured, these parameters are not displayed in the command output. ● Packet type: indicates the protocol type of packets. ● Rate limit: indicates the rate limit. ● Type: indicates the packet type (wired or wireless).
Terminal identify	Whether the terminal identification 2.0 function is enabled. To configure this parameter, run the **terminal-identify disable** command. ● enable: This function is enabled. ● disable
S-IPFPM max user flow	Maximum number of iPCA 2.0 measurement flows for each user. To configure this parameter, run the **s-ipfpm measure max-user-flow** command.
Local management switch	Whether the AP local management function is enabled. To configure this parameter, run the **local-management** command.
Local management IPv4 address	AP local management address. To configure this parameter, run the **local-management ip-address** command.
Service-tunnel-profile	Name of the bound service tunnel profile.

Item	Description
Distribute mode switch	Whether the distributed AP network collaboration function is enabled. To configure this parameter, run the **distribute-mode enable** command.
Self-healing-reset timeout(h)	Time threshold for an AP to restart for self-healing. To configure this parameter, run the **ap-keep-online self-healing-reset** command.
AP keep online switch	Whether the AP always-online function is enabled. To configure this parameter, run the **ap-keep-online disable** command.

11.2.91 display ap-type

Function

The **display ap-type** command displays AP type information.

Format

display ap-type { **all** | **id** *type-id* | **type** *ap-type* }

Parameters

Parameter	Description	Value
all	Displays all the built-in AP types on the device.	-
id *type-id*	Specifies an AP type ID.	The AP type ID must exist.
type *ap-type*	Specifies an AP type name.	The AP type name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view all the built-in AP types on the device and information about APs of the specified type.

Example

Display all the built-in AP types on the device.

```
<HUAWEI> display ap-type all
--------------------------------------------------------------------------------
ID     Type                        Configuration method
--------------------------------------------------------------------------------
......
```

Table 11-105 Description of the **display ap-type all** command output

Item	Description
ID	AP ID.
Type	AP type. The support for AP types depends on device models. For the mapping between AP types and IDs, see the tab page "AP Type Names and IDs" in **Quick Reference for WLAN AP Version Mapping and Models**.
Configuration method	AP type configuration method. • default: The AP type is registered during initialization. • configure(init): The AP type is added using a command, and no APs of such type have been online. • configure(normal): The AP type is added using a command, and the AC has synchronized AP type information from the AP.

Display the AP type with a specified AP type ID.

```
<HUAWEI> display ap-type id 125
--------------------------------------------------------------------------------
Type                          : AirEnginexxxx
AP wired port number                : 5
AP wired port  0 type               : FE
AP wired port  1 type               : FE
AP wired port  0 type               : MultiGE
AP wired port  1 type               : MultiGE
AP wired port  0 type               : XGE
AP Eth-Trunk number                 : 1
Radio number                      : 3
Radio 0 type                    : 802.11bgnax
  Maximal spatial streams           : 4
  Maximal antenna number            : 4
```



```
  Maximal VAP number                  : 16
  Antenna gain                        : 3
  Frequency switching                 : N
  Supported frequency                 : 2.4G
Radio 1 type                          : 802.11anacax
  Maximal spatial streams             : 8
  Maximal antenna number              : 12
  Maximal VAP number                  : 16
  Antenna gain                        : 3
  Frequency switching                 : N
  Dual-5G high/low band support       : High band(100~165)
  Supported frequency                 : 5G
Radio 2 type                          : 802.11anacax
  Maximal spatial streams             : 8
  Maximal antenna number              : 8
  Maximal VAP number                  : 16
  Antenna gain                        : 3
  Frequency switching                 : N
  Dual-5G high/low band support       : Low band(36~64)
  Supported frequency                 : 5G
Maximum station number                : 1152
AP environment high temperature threshold (degree C) : 100
AP CPU high temperature threshold (degree C)         : 110
AP IRF high temperature threshold (degree C)         : 110
AP environment low temperature threshold (degree C)  : -15
AP CPU low temperature threshold (degree C)          : -15
AP IRF low temperature threshold (degree C)          : -15
Outdoor                               : N
BLE                                   : Y
Number of IoT cards                   : 3
PMF                                   : Y
Optical module                        : Y
Optical module information query      : Y
Mesh                                  : Y
WDS                                   : N
Eth-Trunk                             : Y
External antenna                      : N
Frequency fast switching              : N
Radio mode                            : 2radio-standard(default)/3radio/2radio-independent-scan
------------------------------------------------------------------------------
```

Table 11-106 Description of the **display ap-type id** command output

Item	Description
Type	AP type.
AP wired port number	Number of wired interfaces.
AP wired port 0 type	Type of wired interfaces.
AP Eth-Trunk number	Number of Eth-Trunk interfaces.
Radio number	Number of radios.
Radio 0 type	Type of the radio. The value 0 indicates the radio ID.
Maximal spatial streams	Maximum number of spatial streams on the radio.
Maximal antenna number	Maximum number of antennas on the radio.

Item	Description
Maximal VAP number	Maximum number of VAPs on the radio.
Antenna gain	Antenna gain of the radio, in dB. When the antenna gain of an AP is not an integer, the AC rounds the value off and delivers the integer antenna gain. For example, if the 2.4 GHz antenna gain of an AP is 2.5 dB, the 2.4 GHz antenna gain of 3 dB is displayed on the AC.
Frequency switching	Whether the radio can be switched.
Supported frequency	Supported frequency band.
Dual-5G high/low band support	Working frequency band of the 5 GHz radio. ● Low band (36-64): The 5 GHz radio works at a low frequency band. ● High band (100-165): The 5 GHz radio works at a high frequency band. ● All band (36-165): The 5 GHz radio works at any frequency band.
Maximum station number	Maximum number of supported STAs.
AP device high temperature threshold (degree C)	Upper device temperature alarm threshold of an AP. **NOTICE** This parameter is not displayed for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E.
AP environment high temperature threshold (degree C)	Upper ambient temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine central APs.

Item	Description
AP CPU high temperature threshold (degree C)	Upper CPU temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine 9700D-M.
AP NP high temperature threshold (degree C)	Upper NP module temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the AirEngine 9700D-M.
AP IRF high temperature threshold (degree C)	Upper IRF temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E.
AP device low temperature threshold (degree C)	Lower device temperature alarm threshold of an AP. **NOTICE** This parameter is not displayed for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E.
AP environment low temperature threshold (degree C)	Lower ambient temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine central APs.

Item	Description
AP CPU low temperature threshold (degree C)	Lower CPU temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine 9700D-M.
AP NP low temperature threshold (degree C)	Lower NP module temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the AirEngine 9700D-M.
AP IRF low temperature threshold (degree C)	Lower IRF temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E.
Outdoor	Whether the AP is an outdoor AP.
BLE	Whether Bluetooth is supported.
Number of IoT cards	Number of IoT cards.
PMF	Whether PMF is supported.
Optical module	Whether the optical module is supported.
Optical module information query	Whether optical module information can be queried.
Mesh	Whether the Mesh function is supported.
WDS	Whether the WDS function is supported.
Eth-Trunk	Whether the Eth-Trunk is supported.
External antenna	Whether external antennas are supported.
Frequency fast switching	Whether fast radio switching without the need of a restart is supported.

Item	Description
Radio mode	Radio mode supported by an AP. If multiple radio modes are supported, the default radio mode of the AP model is marked as **default**.

11.2.92 display ap-type undefined record

Function

The **display ap-type undefined record** command displays the types of the APs that fail to connect to an AC because the AC does not support these AP types.

Format

display ap-type undefined record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a new AP model cannot connect to the AC, you can check whether the AP type has been created. To list the undefined AP types, run the **display ap-type undefined record** command. Then run the **auto create ap-type** command to automatically import the AP types of these APs.

Example

Display the AP types of the APs that fail to connect to an AC because the AC does not support these AP types.

```
<HUAWEI> display ap-type undefined record
-------------------------------------------------------------------------------
AP type      Type ID     Report AP MAC    Report Time
-------------------------------------------------------------------------------
AP5010DN     29          00e0-fc76-e360   2019-04-28/23:39:00
-------------------------------------------------------------------------------
Total : 1
```


Table 11-107 Description of the **display ap-type undefined record** command output

Item	Description
AP type	AP type.
Type ID	ID of an AP type.
Report AP MAC	MAC address of an AP that fails to connect to the AC the last time because the AC does not support the AP type.
Report Time	Last time when an AP fails to connect to the AC because the AC does not support the AP type.

11.2.93 display ap-type attributes abnormal-check-record

Function

The **display ap-type attributes abnormal-check-record** command displays records of AP attribute check exceptions after an AP type is created.

Format

display ap-type attributes abnormal-check-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When an AP of a new version is connected to an AC, the AC verifies the attributes of the AP to prevent the following problems:

- If the AP attributes defined in the earlier version are modified, for example, a value range is modified, an incompatibility issue may be caused.
- Some attributes of the AP are missing. As a result, the AP fails to connect to the AC.

Example

Display the records of AP attribute check exceptions after an AP type is created.

```
<HUAWEI> display ap-type attributes abnormal-check-record
------------------------------------------------------------------------
AP type          Type ID   Result     Reason
------------------------------------------------------------------------
AP5010DN         29        risky      range conflict
AP6010DN         21        failed     lost-attributes
------------------------------------------------------------------------
Total : 2
```

Table 11-108 Description of the **display ap-type attributes abnormal-check-record** command output

Item	Description
AP type	AP type.
Type ID	ID of an AP type.
Result	AP attribute check result.
Reason	Cause for the check result.

11.2.94 display channel switch-record

Function

The **display channel switch-record** command displays channel switching records on the device.

Format

display channel switch-record { **all** | **calibrate** | **ap-name** *ap-name* **radio** *radio-id* | **ap-id** *ap-id* **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Displays all channel switching records.	-
calibrate	Displays channel switching records for radio calibration.	-
ap-name *ap-name*	Displays channel switching records of the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays channel switching records of a specified AP radio.	The radio ID must exist.

Parameter	Description	Value
ap-id *ap-id*	Displays channel switching records of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check channel switching records on a device.

Run the **display channel switch-record calibrate** command to query channel or power switching records caused by radio calibration to check the calibration results.

Example

Display all channel switching records.

```
<HUAWEI> display channel switch-record all
OldCh/NewCh: Old channel/New channel
OldBw/NewBw: Old bandwidth/New bandwidth
RfID   : Radio ID
------------------------------------------------------------------------------------------------------------------------
AP ID AP name                RfID   OldCh/NewCh      OldBw/NewBw      Switch reason        Switch time
------------------------------------------------------------------------------------------------------------------------
15    AirEngine6760R-51_324033A6 1      -/149            20M/20M          configuration
2020-07-13/14:43:46
------------------------------------------------------------------------------------------------------------------------
Total : 1, printed : 1
```

Table 11-109 Description of the **display channel switch-record all** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
OldCh/NewCh	Channels used before and after switching.
OldBw/NewBw	Bandwidths before and after channel switching.

Item	Description
Switch reason	Reason for channel switching. • calibration: channel switching caused by radio calibration • configuration: channel switching caused by configuration • dfs: channel switching performed to avoid radar channels • dfs (In AC): channel switching caused by channel delivery by the AC to avoid radar channels • dfs recover: channel switching caused by DFS channel switchback • mesh: channel switching caused by channel negotiation on a Mesh network • unsupported: channel switching performed because the AP does not support the channel delivered from the AC • wds: channel switching caused by channel negotiation on a WDS network • iot-notification: channel switching notified by an IoT card • AP sync: channel switching caused by configuration synchronization (through AC-Fit AP channel synchronization) • Poor quality: channel switching caused by radio calibration triggered when the analyzer identifies poor-QoE APs
Switch time	Time when channel switching occurred.

Display channel calibration records.

```
<HUAWEI> display channel switch-record calibrate
PCH : Pre channel
CCH : Current channel
PBW : Pre bandwidth
CBW : Current bandwidth
PE  : Pre EIRP (dBm)
CE  : Current EIRP (dBm)
PRS : Pre RX sensitivity(dBm)
CRS : Current RX sensitivity(dBm)
PR  : Pre RSSI (dBm)
CR  : Current RSSI (dBm)
```



```
RfID: Radio ID
--------------------------------------------------------------------------------------------------------------------------
----
AP ID AP name   RfID  PCH/CCH  PBW/CBW  PE/CE   PRS/CRS    PR/CR    Reason        Time
Trigger ID(Radio)
--------------------------------------------------------------------------------------------------------------------------
----
0     AP1       0     11/6     80M/40M+ 27/127  -95/-82    -32/-40  Period recheck 19:30:00 2016/04/11  -
1     AP2       0     6/11     20M/20M  27/127  -95/-82    -40/-48  Bad env        19:21:53 2016/04/11  3(0)
--------------------------------------------------------------------------------------------------------------------------
----
Total : 2
```

Table 11-110 Description of the **display channel switch-record calibrate** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
PCH/CCH	Channels before and after calibration. **NOTE** PCH/CCH changes may be discontinuous for a radio.
PBW/CBW	Bandwidth before and after calibration.
PE/CE	Power before and after calibration. **NOTE** PE/CE changes may be discontinuous for a radio.
PRS/CRS	Receiver sensitivity values before and after calibration.
PR/CR	Interference values before and after calibration.

Item	Description
Reason	Reason for triggering calibration. • Period recheck: periodic calibration • Bad env: environment deterioration • Non-Wi-Fi report: non-Wi-Fi report • Rogue AP report: rogue AP report • Noise interfere: noise interference • Global plan: network-wide plan • AP online: The AP radio is on, the radio is switched (between 2.4 GHz and 5 GHz bands), the radio working mode changes, or the AP goes online. • AP offline: The AP radio is off, the radio is switched (between 2.4 GHz and 5 GHz bands), the radio working mode changes, or the AP goes offline. • Bad Channel: The channel deteriorates, causing a loss of Beacon frames. • iot-notification: An IoT card notifies calibration. • DFS(In AC): The AC delivers a channel to avoid radar channels. • High interference: Severe interference occurs. • Unknown: unknown reason
Time	Time when calibration is triggered.
Trigger ID(Radio)	ID of the AP (radio) that triggers partial radio calibration. **NOTE** If global radio calibration is triggered, this field displays **-**.

11.2.95 display distribute-ap

Function

The **display distribute-ap** command displays information about RUs.

Format

display distribute-ap { **all** | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-name** *ap-name* | **central-ap-id** *central-ap-id* | **central-ap-mac** *central-ap-mac* | **central-ap-name** *central-ap-name* }

Parameters

Parameter	Description	Value
all	Displays information about all RUs.	-
ap-id *ap-id*	Displays information about the RU of a specified ID.	The RU ID must exist.
ap-mac *ap-mac*	Displays information about the RU of a specified MAC address.	The MAC address must exist.
ap-name *ap-name*	Displays information about the RU of a specified name.	The RU name must exist.
central-ap-id *central-ap-id*	Displays information about the RUs connected to the central AP of a specified ID.	The central AP ID must exist.
central-ap-mac *central-ap-mac*	Displays information about the RUs connected to the central AP of a specified MAC address.	The MAC address of the central AP must exist.
central-ap-name *central-ap-name*	Displays information about the RUs connected to the central AP of a specified name.	The central AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check RU information.

Example

Display information about all RUs.

```
<HUAWEI> display distribute-ap all
Total AP information:
nor : normal          [3]
-------------------------------------------------------------------------------------------------------------
ID   MAC          Name          Group   IP          Type  State  Central-AP ID  Central-AP MAC  Central-AP
name
```



```
-------------------------------------------------------------------------------------------------------------
1    00e0-fc76-e360 00e0-fc76-e360 group1  10.1.1.182 XXXXX nor    0             00e0-fc37-98a0  00e0-
fc37-98a0
2    00e0-fcf5-7280 00e0-fcf5-7280 group   10.1.1.158 XXXXX nor    0             00e0-fc37-98a0  00e0-
fc37-98a0
3    00e0-fcf6-0ce0 ap1           default 10.1.1.181 XXXXX nor    0             00e0-fc37-98a0  00e0-fc37-98a0
-------------------------------------------------------------------------------------------------------------
Total: 3
```

Table 11-111 Description of the **display distribute-ap all** command output

Item	Description
ID	RU ID.
MAC	MAC address of the RU.
Name	Name of the RU.
Group	AP group to which an RU belongs.
IP	IP address of the RU.
Type	RU type.
State	RU state, which is the same as a common AP. For details, see **Table 11-5**.
Central-AP ID	ID of the central AP.
Central-AP MAC	MAC address of the central AP.
Central-AP name	Name of the central AP.

Table 11-112 AP state list

AP State	Description	Possible Cause	Handling Suggestion
commit-failed (cmtfa)	WLAN service configurations fail to be delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are performed for the AP. If the link between the AP and AC is disconnected or the peer end has no response, the AP enters the commit-failed state.	Check the network connection.

AP State	Description	Possible Cause	Handling Suggestion
committing (cmt)	WLAN service configurations are being delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are being delivered to the AP. During this process, the AP is in committing state.	This is a normal state, and no action is required.
config (cfg)	WLAN service configurations are being delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. During this process, the AP is in config state.	This is a normal state, and no action is required.
config-failed (cfgfa)	WLAN service configurations fail to be delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. If the configuration delivery fails due to various reasons (such as link disconnection), the AP enters the config-failed state.	Check the network connection.
download (dload)	An AP is in upgrade state.	When an AP is performing an upgrade, it enters the download state.	When the AP upgrade is complete, check the AP state.

AP State	Description	Possible Cause	Handling Suggestion
fault	An AP fails to go online.	An AP fails to go online, which is usually caused by the following: • The AP fails to obtain an IP address or obtains an incorrect IP address. • The network between the AP and AC is faulty. • The AP fails to be authenticated. • The number of APs on an AC has reached the maximum value. • The AP is faulty. • In dual-link cold backup or N+1 backup scenario, if the link between the active and standby ACs is established properly, an AP that goes online on the active AC is in fault state on the standby AC.	Handle the AP online failure. For details, see **An AP Fails to Go Online on the AC** in the *Troubleshooting Guide*.

AP State	Description	Possible Cause	Handling Suggestion
idle	It is the initialization state of an AP before it establishes a link with the AC for the first time.	When an AP has not established a CAPWAP link with the AC, the MAC address and SN of an AP that is added offline are different from the actual MAC address and SN of the AP, or the AC cannot manage an AP due to license resource insufficiency, the AP enters the idle state.	Perform the following operations. Check whether the AP is connected to the network. If the AP connection is normal, go to next step. Check the MAC address and SN of the AP that is added offline are different from the actual MAC address and SN of the AP. If not, perform the following operations: 1. Run the **display ap all** command to check AP information. 2. Run the **undo ap** { **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** } command to delete the AP. 3. Run the **ap-id** *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }] or **ap-mac** *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*] command to add correct AP information. If the fault persists, expand the license capacity. Note that RUs managed by the AC do not occupy

AP State	Description	Possible Cause	Handling Suggestion
			license resources of the AC.
name-conflicted (namec)	The name of an AP conflicts with that of an existing AP.	The name of an AP conflicts with the name of another AP that has been online on the same AC.	Run the **ap-rename ap-id** *ap-id* **new-name** *ap-new-name* command to change the AP name.
normal (nor)	An AP is working properly.	An AP successfully goes online on an AC.	This is a normal state, and no action is required.
standby (stdby)	An AP is in normal state on the standby AC.	In the HSB scenario, if the link between the master and backup ACs is established properly, an AP is in standby state on the backup AC and in normal state on the master AC.	This is a normal state, and no action is required.
ver-mismatch (vmiss)	The version of an AP does not match that of an AC on which the AP is about to go online.	The versions of the AP and AC do not match.	Log in to Huawei technical support website and download the release notes. Based on the version mapping, upgrade the AP or AC to the matching version. • Enterprise technical support website: **https://support.huawei.com/enterprise** • Carrier technical support website: **https://support.huawei.com**

AP State	Description	Possible Cause	Handling Suggestion
countryCode-mismatch (cmiss)	The country codes of the AP and AC do not match.	The AP's current version does not support the country code configured on the AC. The country code of the AP is locked, and the country code configured on the AC is not supported.	The AP does not support the country code. Upgrade the AP or modify the country code configuration on the AC. The country code of the AP is locked. Replace the AP or change the country code on the AC to be the same as that of the AP.
type-mismatch (tmiss)	The AP type does not match that configured on the AC.	The AP type configured on the AC did not match the actual AP type.	Change the AP type configured on the AC.
unauth	An AP is not authenticated.	The AP fails to be authenticated.	Run the **display ap unauthorized record** command to query authenticated APs. Run the **ap-confirm** command to confirm unauthenticated APs and allow them to go online.

11.2.96 display mac-address ap-all

Function

The **display mac-address ap-all** command displays MAC address entries on all APs.

Format

display mac-address *mac-address* [**verbose**] **ap-all**

Parameters

Parameter	Description	Value
mac-address	Displays MAC address entries on all APs.	The value is in H-H-H format. An H contains four hexadecimal numbers.
verbose	Displays detailed information of the dynamic entries. If *verbose* is not specified, brief information about MAC address entries is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When errors or attacks occur on the network, you can run the **display mac-address ap-all** command to locate the attack sources based on the displayed MAC addresses.

Example

Display dynamic MAC address entries of all APs.

```
<HUAWEI> display mac-address 00e0-fc09-bcf9 ap-all
Info: Waiting for AP response...done.
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI       Learned-From            Type       AP ID
--------------------------------------------------------------------------------
00e0-fc09-bcf9 1/-            GigabitEthernet0/0/0    dynamic    1
00e0-fc09-bcf9 1/-            GigabitEthernet0/0/0    dynamic    0
--------------------------------------------------------------------------------
Total: 2
```

Table 11-113 Description of the **display mac-address** *mac-address* **ap-all** command output

Item	Description
MAC Address	MAC address.
VLAN/VSI	ID of the VLAN or name of the VSI that a MAC address belongs to.

Item	Description
Learned-From	Interface on which the MAC address is learned.
Type	Type of a MAC address entry.
AP ID	AP ID.

11.2.97 display mac-address { ap-id | ap-name }

Function

The **display mac-address** { **ap-id** | **ap-name**} command displays all dynamic, dynamic secure, and sticky MAC address entries on an AP's wired interface.

Format

display mac-address { **ap-id** *ap-id* | **ap-name** *ap-name* } *interface-type interface-number*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays all dynamic, dynamic secure, and sticky MAC address entries on wired interfaces of the AP with the specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays all dynamic, dynamic secure, and sticky MAC address entries on wired interfaces of the AP with the specified name.	The AP name must exist.
interface-type interface-number	Displays all dynamic, dynamic secure, and sticky MAC address entries on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the number of the outbound interface.	The following types of outbound interfaces are supported: • Eth-Trunk • Ethernet • Gigabitethernet • MultiGE • XGigabitethernet

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mac-address** { **ap-id** | **ap-name**} command to check all dynamic, dynamic secure, and sticky MAC address entries on an AP's wired interface, including the MAC addresses and VLANs that the AP learns on specified interfaces.

Example

Display all dynamic, dynamic secure, and sticky MAC address entries on wired interfaces of the AP with ID 1.

```
<HUAWEI> display mac-address ap-id 1 ethernet 0
------------------------------------------------------------
MAC Address    VLAN/VSI   Learned-From        Type
------------------------------------------------------------
00e0-fc54-5a80 1/-        Ethernet0/0/0       dynamic
------------------------------------------------------------
Total: 1
```

Table 11-114 Description of the **display mac-address ap-id** *ap-id interface-type interface-number* command output

Item	Description
MAC Address	MAC address.
VLAN/VSI	VLAN or VSI to which the device belongs.
Learned-From	Interface on which the MAC address is learned.
Type	Type of a MAC address entry.

11.2.98 display port-link-profile

Function

The **display port-link-profile** command displays reference and configuration information about an AP wired port link profile.

Format

display port-link-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP wired port link profiles.	-
name *profile-name*	Displays information about a specified AP wired port link profile.	The AP wired port link profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display port-link-profile** command to view configuration and reference information about an AP wired port link profile.

Example

Display information about all AP wired port link profiles.

```
<HUAWEI> display port-link-profile all
------------------------------------------------------------
Profile name                  Reference
------------------------------------------------------------
default                       1
port-link-profile-1           0
------------------------------------------------------------
Total: 2
```

Table 11-115 Description of the **display port-link-profile all** command output

Item	Description
Profile name	Name of an AP wired port link profile.
Reference	Number of times an AP wired port link profile is referenced.

Display information about the AP wired port link profile **default**.

```
<HUAWEI> display port-link-profile name default
------------------------------------------------------------------------------
LLDP enable                   : enable
Management address            : enable
Port description              : enable
System capability             : enable
```



```
System description              : enable
System name                     : enable
802.3 TLV power                 : enable
802.3 TLV power format          : 802.3bt
Legacy TLV four pair power      : enable
Legacy TLV power capability     : enable
CRC error alarm                 : disable
CRC error high threshold(1/10000): 50
CRC error Low threshold(1/10000) : 20
PoE enable                      : enable
PoE legacy                      : disable
PoE priority                    : low
PoE force power                 : disable
Shutdown switch                 : disable
Speed(Mbit/s)                   : -
------------------------------------------------------------------------------
```

Table 11-116 Description of the **display port-link-profile name** *profile-name* command output

Item	Description
LLDP enable	Whether LLDP is enabled on an AP's wired interface. To configure the parameter, run the **lldp enable** command.
Management address	Whether an AP's wired interface is allowed to advertise the Management-address TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
Port description	Whether an AP's wired interface is allowed to advertise the Port-description TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
System capability	Whether an AP's wired interface is allowed to advertise the System-capability TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
System description	Whether an AP's wired interface is allowed to advertise the System-description TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.

Item	Description
System name	Whether an AP's wired interface is allowed to advertise the System-name TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
802.3 TLV power	Whether an AP's wired interface is allowed to advertise the Power via MDI TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
802.3 TLV power format	802.3 Power via MDI TLV advertised by an AP's wired interface. ● 802.1ab: The 802.3 Power via MDI TLV sent by the interface conforms to 802.1ab. ● 802.3at: The 802.3 Power via MDI TLV sent by the interface conforms to 802.3at. ● 802.3bt: The 802.3 Power via MDI TLV sent by the interface conforms to 802.3bt. ● -: Default value. To configure the parameter, run the **lldp dot3-tlv power (AP wired port link profile view)** command.
Legacy TLV four pair power	Whether an AP's wired interface is allowed to advertise Cisco's customized TLVs. To configure the parameter, run the **lldp tlv-enable legacy-tlv four-pair-power (AP wired port link profile view)** command.
Legacy TLV power capability	Whether the supported power capability is carried in LLDP packets sent by an AP. To configure the parameter, run the **lldp tlv-enable legacy-tlv power-capability (AP wired port link profile view)** command.

Item	Description
CRC error alarm	Whether the alarm function for CRC errors is enabled on an AP's wired interface. To configure the parameter, run the **crc-alarm enable** command.
CRC error high threshold(1/10000)	Alarm threshold for CRC errors on an AP's wired interface. To configure the parameter, run the **crc-alarm enable** command.
CRC error Low threshold(1/10000)	Clear alarm threshold for CRC errors on an AP's wired interface. To configure the parameter, run the **crc-alarm enable** command.
PoE enable	Whether the PoE function is enabled on the AP's interfaces. To configure the parameter, run the **poe disable (AP wired port link profile view)** command.
PoE legacy	Whether PD compatibility check is enabled on the AP. To configure the parameter, run the **poe legacy enable (AP wired port link profile view)** command.
PoE priority	Power priority of PoE interfaces on the AP. To configure the parameter, run the **poe priority (AP wired port link profile view)** command.
PoE force power	Whether forcible PoE power supply is enabled on the AP's interfaces. To configure the parameter, run the **poe force-power (AP wired port link profile view)** command.
Shutdown switch	Whether the AP's wired interface function is disabled. To configure the parameter, run the **shutdown (AP wired port link profile view)** command.

Item	Description
Speed(Mbit/s)	Rate of the AP's wired interface in non-auto negotiation mode. To configure the parameter, run the **speed (AP wired port link profile view)** command.

11.2.99 display provision-ap parameter-list

Function

The **display provision-ap parameter-list** command displays AP provisioning parameters in the AP provisioning view.

Format

display provision-ap parameter-list

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running the **commit** command to deliver the AP provisioning parameters configured in the AP provisioning view, you can run the **display provision-ap parameter-list** command to check whether the parameters are correct and complete.

If a parameter is displayed as **-** in the command output, the parameter of the APs is not changed after the configuration is committed.

Example

Display AP provisioning parameters in the AP provisioning view.

```
<HUAWEI> display provision-ap parameter-list
--------------------------------------------------------------------------------
AP mode               : -
AP name               : -
AP address mode         : -
IPv4 address          : -
IPv4 mask address       : -
```



```
IPv4 gateway address     : -
IPv4 AC list             : -
Management Vlan          : 2
DTLS server-auth         : enable
DTLS server-auth cn list : -
--------------------------------------------------------------------------------
```

Table 11-117 Description of the **display provision-ap parameter-list** command output

Item	Description
AP mode	AP mode. To set this parameter, run the **ap-mode** command.
AP name	AP name. To configure this parameter, run the **ap-name (AP provisioning view)** command.
AP address mode	Mode in which an AP obtains an IP address. To configure this parameter, run the **address-mode (AP provisioning view)** command.
IPv4 address	Static IPv4 address of an AP. To configure this parameter, run the **ip-address (AP provisioning view)** command.
IPv4 mask address	Static IPv4 address mask of an AP. To configure this parameter, run the **ip-address (AP provisioning view)** command.
IPv4 gateway address	IPv4 address gateway of the AP. To configure this parameter, run the **ip-address (AP provisioning view)** command.
IPv4 AC list	AC IPv4 address list of an AP. To configure this parameter, run the **ac-list (AP provisioning view)** command.
Management Vlan	Management VLAN tag carried in CAPWAP packets sent from the AP's wired interface. To configure this parameter, run the **management-vlan** command.

Item	Description
DTLS server-auth	Whether the AC authentication function is enabled for the AP. To configure this parameter, run the **capwap dtls server-auth (AP provisioning view)** command.
DTLS server-auth cn list	CN field in the AC certificate to be authenticated by the AP. To configure this parameter, run the **capwap dtls server-auth cn (AP provisioning view)** command.

11.2.100 display references ap-pki-profile

Function

The **display references ap-pki-profile** command displays reference information about an AP PKI realm profile.

Format

display references ap-pki-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the profile name.	The profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view reference information about an AP PKI realm profile.

Example

Display reference information about an AP PKI realm profile.


```
<HUAWEI> display references ap-pki-profile name default
Total: 5
--------------------------------------------------------------
Reference type          Reference name
--------------------------------------------------------------
ap-group                default
ap-group                mytest
ap-id                   69
ap-id                   70
ap-id                   72
--------------------------------------------------------------
```

Table 11-118 Description of the **display references ap-pki-profile** command output

Item	Description
Reference type	Profile binding type. The options are as follows: • **ap-group**: bound to an AP group • **ap-id**: bound to an AP The **ap-group** and **ap-id** types are available.
Reference name	Name of an AP group or ID of an AP to which the profile is bound.

11.2.101 display references ap-system-profile

Function

The **display references ap-system-profile** command displays reference information about an AP system profile.

Format

display references ap-system-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified AP system profile.	The AP system profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references ap-system-profile** command to view reference information about an AP system profile.

Example

Display reference information of the AP system profile **default**.

```
<HUAWEI> display references ap-system-profile name default
------------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------------
AP group                    default
------------------------------------------------------------------------------
Total: 1
```

Table 11-119 Description of the **display references ap-system-profile** command output

Item	Description
Reference type	Type of the profile by which an AP system profile is referenced.
Reference name	Name of the profile by which an AP system profile is referenced.

11.2.102 display references port-link-profile

Function

The **display references port-link-profile** command displays reference information about an AP wired port link profile.

Format

display references port-link-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified AP wired port link profile.	The AP wired port link profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references port-link-profile** command to view reference information about an AP wired port link profile.

Example

Display reference information about the AP wired port link profile **default**.

```
<HUAWEI> display references port-link-profile name default
------------------------------------------------------------------------
Reference type                Reference name
------------------------------------------------------------------------
AP wiredport profile          wired-port1
------------------------------------------------------------------------
Total:1
```

Table 11-120 Description of the **display references port-link-profile** command output

Item	Description
Reference type	Type of the profile by which an AP wired port link profile is referenced.
Reference name	Name of the profile by which an AP wired port link profile is referenced.

11.2.103 display references wired-port-profile

Function

The **display references wired-port-profile** command displays reference information about an AP wired port profile.

Format

display references wired-port-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified AP wired port profile.	The AP wired port profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wired-port-profile** command to view reference information about an AP wired port profile.

Example

Display reference information about the AP wired port profile **default**.

```
<HUAWEI> display references wired-port-profile name default
--------------------------------------------------------------------------------
Reference type     Reference name                Reference port
--------------------------------------------------------------------------------
AP group           default                       Ethernet0
AP group           default                       Ethernet1
AP group           default                       Ethernet2
AP group           default                       Ethernet3
AP group           default                       GigabitEthernet0
AP group           default                       GigabitEthernet1
AP group           default                       GigabitEthernet2
AP group           default                       GigabitEthernet3
AP group           default                       GigabitEthernet4
AP group           default                       GigabitEthernet5
AP group           default                       GigabitEthernet6
AP group           default                       GigabitEthernet7
AP group           default                       GigabitEthernet8
AP group           default                       GigabitEthernet9
AP group           default                       GigabitEthernet10
AP group           default                       GigabitEthernet11
AP group           default                       GigabitEthernet12
AP group           default                       GigabitEthernet13
AP group           default                       GigabitEthernet14
AP group           default                       GigabitEthernet15
AP group           default                       GigabitEthernet16
AP group           default                       GigabitEthernet17
AP group           default                       GigabitEthernet18
AP group           default                       GigabitEthernet19
AP group           default                       GigabitEthernet20
AP group           default                       GigabitEthernet21
AP group           default                       GigabitEthernet22
AP group           default                       GigabitEthernet23
AP group           default                       GigabitEthernet24
AP group           default                       GigabitEthernet25
AP group           default                       GigabitEthernet26
AP group           default                       GigabitEthernet27
AP group           default                       MultiGE0
```



```
AP group        default                 XGigabitEthernet0
AP group        default                 XGigabitEthernet1
AP group        default                 XGigabitEthernet2
AP group        default                 XGigabitEthernet3
AP group        default                 Ethernet-Trunk0
------------------------------------------------------------------------------
Total: 38
```

Table 11-121 Description of the **display references wired-port-profile** command output

Item	Description
Reference type	Type of the profile by which an AP wired port profile is referenced.
Reference name	Name of the profile by which an AP wired port profile is referenced.
Reference port	Interface by which an AP wired port profile is referenced.

11.2.104 display wired-port-profile

Function

The **display wired-port-profile** command displays reference and configuration information about an AP wired port profile.

Format

display wired-port-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP wired port profiles.	-
name *profile-name*	Displays information about a specified AP wired port profile.	The AP wired port profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about an AP wired port profile.

Example

Display information about all AP wired port profiles.

```
<HUAWEI> display wired-port-profile all
------------------------------------------------------------
Profile name                Reference
------------------------------------------------------------
default                     1
wired-port-profile-1        0
------------------------------------------------------------
Total: 2
```

Table 11-122 Description of the **display wired-port-profile all** command output

Item	Description
Profile name	Name of an AP wired port profile.
Reference	Number of times an AP wired port profile is referenced.

Display information about the AP wired port profile **default** (Eth-trunk is not configured).

```
<HUAWEI> display wired-port-profile name default
------------------------------------------------------------------------------
Port link profile                    : default
Description                          :
STP                                  : disable
Port work mode                       : -
Port Tagged VLAN                     : -
Port untagged VLAN                   : 1
Port PVID VLAN                       : -
User isolate mode                    : disable
DHCP trust port                      : enable
ND trust port                        : enable
IPSG switch                          : disable
DAI switch                           : disable
STP auto shutdown switch             : disable
Auto shutdown recovery time          : 600
Learn client IPv4 address switch     : disable
Learn client IPv6 address switch     : disable
IGMP-Snooping switch                 : disable
MLD-Snooping switch                  : disable
Port security switch                 : disable
Port security sticky MAC             : disable
Port security maximum MAC            : 1
Port security protect action         : restrict
Traffic optimize TCP adjust MSS(bytes)        : -
Traffic optimize broadcast suppression(pps)   : -
Traffic optimize unicast suppression(pps)     : -
Traffic optimize multicast suppression(pps)   : -
------------------------------------------------------------------------------
Traffic Type              Direction  AppliedRecord
------------------------------------------------------------------------------
traffic-filter            inbound    IPv4 ACL 3012
```



```
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Traffic Type                    Direction  RemarkType  RemarkValue  AppliedRecord
-------------------------------------------------------------------------------
traffic-remark                   outbound   802.1p      2            IPv4 ACL 3011
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
```

Display information about the AP wired port profile **dj** (Eth-trunk is configured).

```
<HUAWEI> display wired-port-profile name dj
-------------------------------------------------------------------------
Port link profile          : default
Description                :
Ethernet trunk ID            : 0
-------------------------------------------------------------------------
```

Table 11-123 Description of the **display wired-port-profile name** *profile-name* command output

Item	Description
Port link profile	Name of the AP wired port link profile referenced by an AP wired port profile. To configure the parameter, run the **port-link-profile (AP wired port profile view)** command.
Description	Interface description. To configure the parameter, run the **description (AP wired port profile view)** command.
STP	STP status on a wired interface. To configure the parameter, run the **stp enable (AP wired port profile view)** command.
Port work mode	Working mode of a wired interface. ● root: indicates the root mode. ● endpoint: indicates the endpoint mode. ● middle: indicates the middle mode. ● -: indicates that the working mode of wired interfaces is not changed. To configure the parameter, run the **mode (AP wired port profile view)** command.
Port Tagged VLAN	VLAN to which a wired interface is added in tagged mode. To configure the parameter, run the **vlan (AP wired port profile view)** command.

Item	Description
Port untagged VLAN	VLAN to which a wired interface is added in untagged mode. To configure the parameter, run the **vlan (AP wired port profile view)** command.
Port PVID VLAN	PVID of a wired interface. To configure the parameter, run the **vlan pvid (AP wired port profile view)** command.
User isolate mode	User isolation status on a wired interface. To configure the parameter, run the **user-isolate (AP wired port profile view)** command.
DHCP trust port	Status of the DHCP trusted interface function. To configure the parameter, run the **dhcp trust port** command.
ND trust port	Status of the ND trusted interface function. To configure the parameter, run the **nd trust port** command.
Ethernet trunk ID	ID of the Eth-Trunk interface.
IPSG switch	Whether IP source guard (IPSG) is enabled on an AP's wired interface. To configure the parameter, run the **ipsg enable (AP wired port profile view)** command.
DAI switch	Whether DAI is enabled on an AP's wired interface. To configure the parameter, run the **dai enable (AP wired port profile view)** command.
STP auto shutdown switch	Whether STP-triggered port shutdown is enabled on an AP's wired interface. To configure the parameter, run the **stp auto-shutdown enable (AP wired port profile view)** command.

Item	Description
Auto shutdown recovery time	Recovery time of the shutdown port triggered by STP. To configure the parameter, run the **stp auto-shutdown recovery-time (AP wired port profile view)** command.
Learn client IPv4 address switch	Whether terminal IPv4 address learning is enabled on an AP's wired interface. To configure the parameter, run the **learn-client-address enable (AP wired port profile view)** command.
Learn client IPv6 address switch	Whether terminal IPv6 address learning is enabled on an AP's wired interface. To configure the parameter, run the **learn-client-address enable (AP wired port profile view)** command.
IGMP-Snooping switch	Whether IGMP snooping is enabled on an AP's wired interface. To configure the parameter, run the **igmp-snooping enable (AP wired port profile view)** command.
MLD-Snooping switch	Whether MLD snooping is enabled on an AP's wired interface. To configure the parameter, run the **mld-snooping enable (AP wired port profile view)** command.
Port security switch	Whether port security is enabled on an AP's wired interface. To configure the parameter, run the **port-security enable (AP wired port profile view)** command.
Port security sticky MAC	Whether the port security and sticky MAC functions are enabled on an AP's wired interface. To configure the parameter, run the **port-security mac-address sticky (AP wired port profile view)** command.

Item	Description
Port security maximum MAC	Maximum number of secure MAC addresses that can be learned by an interface. To configure the parameter, run the **port-security max-mac-num (AP wired port profile view)** command.
Port security protect action	Protection action to be taken when the number of secure MAC addresses learned by an interface exceeds the limit. • protect: The interface discards packets with source MAC addresses that are not in the MAC address table. • restrict: The interface discards packets with source MAC addresses that are not in the MAC address table and sends a trap message. To configure the parameter, run the **port-security protect-action (AP wired port profile view)** command.
Traffic optimize TCP adjust MSS(bytes)	Maximum segment size (MSS) of TCP packets on an AP's wired interface. To configure the parameter, run the **traffic-optimize tcp adjust-mss** command.
Traffic optimize broadcast suppression(pps)	Maximum broadcast traffic volume that can be received on an AP's wired interface. To configure the parameter, run the **traffic-optimize (AP wired port profile view)** command.
Traffic optimize unicast suppression(pps)	Maximum unknown unicast traffic volume that can be received on an AP's wired interface. To configure the parameter, run the **traffic-optimize (AP wired port profile view)** command.
Traffic optimize multicast suppression(pps)	Maximum multicast traffic volume that can be received on an AP's wired interface. To configure the parameter, run the **traffic-optimize (AP wired port profile view)** command.

Item	Description
Traffic Type	ACL-based packet filtering and re-marking implemented by the AP wired port. • traffic-filter • traffic-remark
Direction	Incoming or outgoing packets.
AppliedRecord	IPv4/IPv6/L2 packet filtering and re-marking based on ACLs.
RemarkType	Protocol type. • dscp • dot1p
RemarkValue	Protocol type value. • dscp: 0-63 • dot1p: 0-7

11.2.105 display wlan ble-link-info

Function

The **display wlan ble-link-info** command displays connection information about the Bluetooth-based air interface on an AP.

NOTE

The following models do not support the Bluetooth serial port function:

- AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
- AirEngine 5762-10 and AirEngine 5762-10SW
- AirEngine 9700D-M and AirEngine 9700D-M1

Format

display wlan ble-link-info { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check connection information about the Bluetooth-based air interface on an AP.

Example

Display connection information about the Bluetooth-based air interface on the AP named **ap1**.

```
<HUAWEI> display wlan ble-link-info ap1
Info: This operation may take a few seconds. Please wait for a moment.done.
--------------------------------------------------------------------------------
BLE access MAC                  : xxxx-xxxx-xxxx
Status                          : paired
Link status changed time        : 2019-04-11  09:12:46
--------------------------------------------------------------------------------
```

Table 11-124 Description of the **display wlan ble-link-info** command output

Item	Description
BLE access MAC	MAC address of a STA accessed through Bluetooth. This address is randomly generated when the STA establishes a Bluetooth connection with the AP.
Status	Bluetooth connection status between a STA and the AP. • link established: The link is established between the STA and AP. • paired: The STA and AP are successfully paired.
Link status changed time	Time when the connection status is updated.

11.2.106 display wlan console ble statistics

Function

The **display wlan console ble statistics** command displays statistics about Bluetooth-based console port login on an AP.

NOTE

The following models do not support the Bluetooth serial port function:

- AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
- AirEngine 5762-10 and AirEngine 5762-10SW
- AirEngine 9700D-M and AirEngine 9700D-M1

Format

display wlan console ble statistics { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check statistics about Bluetooth-based console port login on an AP.

Example

Display statistics about Bluetooth-based console port login on the AP named **huawei**.

```
<HUAWEI> display wlan console ble statistics ap-name huawei
Info: This operation may take a few seconds. Please wait for a moment.done.
------------------------------------------------------------------------------
AP ID                              : 0
AP Name                            : huawei
Air Frame Received (Packets)       : 11
Air Traffic Received (Bytes)       : 11
Air Frame Send (Packets)           : 8
Air Traffic Send (Bytes)           : 55
------------------------------------------------------------------------------
```


Table 11-125 Description of the **display wlan console ble statistics** command output

Item	Description
AP ID	AP ID.
AP Name	AP name.
Air Frame Received (Packets)	Number of received air interface frames.
Air Traffic Received (Bytes)	Amount of received air interface traffic.
Air Frame Send (Packets)	Number of sent air interface frames.
Air Traffic Send (Bytes)	Amount of sent air interface traffic.

11.2.107 disk-usage threshold

Function

The **disk-usage threshold** command sets the disk usage alarm threshold of APs.

The **undo disk-usage threshold** command restores the default disk usage alarm threshold of APs.

The default disk usage alarm threshold of APs is 95.

Format

disk-usage threshold *threshold*

undo disk-usage threshold

Parameters

Parameter	Description	Value
threshold	Specifies a disk usage alarm threshold of APs.	The value is an integer that ranges from 6 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **disk-usage threshold** command to set the disk usage alarm threshold of APs. The corresponding alarm clear threshold equals the specified alarm threshold minus 5. This configuration is delivered to APs using this AP system profile view.

- When the disk usage of APs exceeds the current alarm threshold, the APs report an alarm to the AC, which displays alarm information.
- When the disk usage of APs falls below the current alarm threshold, the APs report a clear alarm to the AC, which displays clear alarm information.

Example

Set the disk usage alarm threshold of APs to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] disk-usage threshold 60
```

11.2.108 eapol-response dest-address transform-condition

Function

The **eapol-response dest-address transform-condition** command specifies the EAPOL-response packets to be encapsulated by an AP.

The **undo eapol-response dest-address transform-condition** command restores the default settings.

By default, an AP encapsulates only the EAPOL-response packets with the destination MAC addresses being the AP's BSSID.

Format

eapol-response dest-address transform-condition { **always** | **equal-bssid** }

undo eapol-response dest-address transform-condition

Parameters

Parameter	Description	Value
always	Configures the AP to encapsulate all EAPOL-response packets.	-
equal-bssid	Configures the AP to encapsulate only the EAPOL-response packets with the destination MAC address being the AP's BSSID.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, the destination MAC addresses of the EAPOL-response packets sent by some STAs are APs' BSSIDs, but the destination MAC addresses of the EAPOL-response packets sent by other STAs are not APs' BSSIDs. You need to run this command to specify the EAPOL-response packets to be encapsulated.

Example

Configure the AP to encapsulate all EAPOL-response packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] eapol-response dest-address transform-condition always
```

11.2.109 eapol-response dest-address transform-to

Function

The **eapol-response dest-address transform-to** command configures an AP to encapsulate EAPOL-response packets into broadcast, multicast, or unicast packets.

The **undo eapol-response dest-address transform-to** command restores the default settings.

By default, an AP encapsulates EAPOL-response packets into unicast packets and actively learns the destination MAC address.

Format

eapol-response dest-address transform-to { **broadcast** | **multicast** | **mac** *mac-address* | **learning** }

undo eapol-response dest-address transform-to

Parameters

Parameter	Description	Value
broadcast	Configures an AP to encapsulate EAPOL-response packets into broadcast packets.	-

Parameter	Description	Value
multicast	Configures an AP to encapsulate EAPOL-response packets into multicast packets.	-
mac *mac-address*	Configures an AP to encapsulate EAPOL-response packets into unicast packets with a specified destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
learning	Configures an AP to encapsulate EAPOL-response packets into unicast packets and actively learn the destination MAC address.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

- If the authentication server can only process EAP multicast packets, configure the AP to encapsulate EAPOL-response packets into multicast packets.
- If the authentication server can only process EAP broadcast packets, configure the AP to encapsulate EAPOL-response packets into broadcast packets.
- If the authentication server can only process EAP unicast packets, configure the AP to encapsulate EAPOL-response packets into unicast packets. When the AP is configured to encapsulate EAPOL-response packets into unicast packets, a unicast MAC address must be configured.

Example

Configure an AP to encapsulate EAPOL-response packets into broadcast packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] eapol-response dest-address transform-to broadcast
```


11.2.110 eapol-start dest-address transform-condition

Function

The **eapol-start dest-address transform-condition** command specifies the EAPOL-start packets to be encapsulated by an AP.

The **undo eapol-start dest-address transform-condition** command restores the default settings.

By default, an AP encapsulates only the EAPOL-start packets with the destination MAC addresses being the AP's BSSID.

Format

eapol-start dest-address transform-condition { **always** | **equal-bssid** }

undo eapol-start dest-address transform-condition

Parameters

Parameter	Description	Value
always	Configures the AP to encapsulate all EAPOL-start packets.	-
equal-bssid	Configures the AP to encapsulate only the EAPOL-start packets with the destination MAC address being the AP's BSSID.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During 802.1X authentication, the destination MAC addresses of the EAPOL-start packets sent by some STAs are APs' BSSIDs, but the destination MAC addresses of the EAPOL-start packets sent by other STAs are not APs' BSSIDs. You need to run this command to specify the EAPOL-start packets to be encapsulated.

Precautions

The packet types specified by the **eapol-start dest-address transform-condition** and **eapol-start dest-address transform-to** commands must be the same.

Example

Configure the AP to encapsulate all EAPOL-start packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] eapol-start dest-address transform-condition always
```

11.2.111 eapol-start dest-address transform-to

Function

The **eapol-start dest-address transform-to** command configures an AP to encapsulate EAPOL-start packets into broadcast, multicast, or unicast packets.

The **undo eapol-start dest-address transform-to** command restores the default settings.

By default, an AP encapsulates EAPOL-start packets into multicast packets.

Format

eapol-start dest-address transform-to { **broadcast** | **multicast** | **mac** *mac-address* }

undo eapol-start dest-address transform-to

Parameters

Parameter	Description	Value
broadcast	Configures an AP to encapsulate EAPOL-start packets into broadcast packets.	-
multicast	Configures an AP to encapsulate EAPOL-start packets into multicast packets.	-
mac *mac-address*	Configures an AP to encapsulate EAPOL-start packets into unicast packets.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

- If the authentication server can only process EAP multicast packets, configure the AP to encapsulate EAPOL-start packets into multicast packets.
- If the authentication server can only process EAP broadcast packets, configure the AP to encapsulate EAPOL-start packets into broadcast packets.
- If the authentication server can only process EAP unicast packets, configure the AP to encapsulate EAPOL-start packets into unicast packets. When the AP is configured to encapsulate EAPOL-start packets into unicast packets, a unicast MAC address must be configured.

Example

Configure an AP to encapsulate EAPOL-start packets into broadcast packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] eapol-start dest-address transform-to broadcast
```

11.2.112 eth-trunk (AP wired port profile view)

Function

The **eth-trunk** command adds an AP interface to an Eth-Trunk.

The **undo eth-trunk** command removes an AP interface from an Eth-Trunk.

By default, an AP interface is not added to any Eth-Trunk.

Format

eth-trunk *trunk-id*

undo eth-trunk

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is 0 or 1.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve the connection reliability and increase the bandwidth, you can run this command to bind multiple interfaces into an Eth-Trunk.

Prerequisites

The physical interface to be added to an Eth-Trunk cannot have other configurations. Before adding a physical interface to an Eth-Trunk, clear all configurations on it except the interface status, descriptions, LLDP function, and alarm function for CRC errors.

Precautions

- After the configuration, you need to restart the AP to make the configured Eth-Trunk on the AP's wired interfaces take effect.
- APs that have only one physical uplink network interface do not support this command.
- Downlink interfaces on an AP do not support the Eth-Trunk function.
- Member interfaces in an Eth-Trunk do not support the PVID or user isolation configuration.
- For an AP that supports only one Eth-Trunk, the configuration takes effect only when the Eth-Trunk ID is set to 0.
- If a member interface of an Eth-Trunk is connected to a peer end, the peer interface directly connected to the local interface must also be a member interface of an Eth-Trunk.
- An Eth-Trunk cannot be added to another Eth-Trunk.
- Do not configure any member interface of an Eth-Trunk as an observing port. If this cannot be avoided, ensure that the bandwidth of service traffic on the member interface and the bandwidth of the mirrored traffic do not exceed the bandwidth limit of the interface.
- An Ethernet interface can be added to only one Eth-Trunk. To add the Ethernet interface in an Eth-Trunk to another Eth-Trunk, delete it from the original Eth-Trunk first.
- After an interface is added to an Eth-Trunk, MAC address entries and ARP entries are learned based on the Eth-Trunk but not based on member interfaces.

NOTE

The Eth-Trunk function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (except AirEngine 5761S-12, AirEngine 5761-12, and AirEngine 5761S-13)
- AirEngine 8771-X1T
- AirEngine 9700D-S (including matching ORUs)
- AirEngine series central APs

Example

Add the AP interface to Eth-Trunk 0.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] eth-trunk 0
```

11.2.113 high-temperature threshold

Function

The **high-temperature threshold** command sets an upper device, ambient, CPU, or NP module temperature alarm threshold for APs.

The **undo high-temperature threshold** command restores the default upper device, ambient, CPU, or NP module temperature alarm threshold of APs.

Table 11-126 Default upper temperature alarm threshold for APs

AP Model	Default Value (°C)
AirEngine 9700D-M1 (AP device/ ambient)	63/54

NOTE

This command is not supported by the following models:

- AirEngine series APs

Format

high-temperature [**ap-environment** | **cpu** | **np**] **threshold** *threshold*

undo high-temperature [**ap-environment** | **cpu** | **np**] **threshold**

Parameters

Parameter	Description	Value
ap-environment	Indicates the ambient temperature.	-
cpu	Indicates the CPU temperature.	-
np	Indicates the NP module temperature.	-

Parameter	Description	Value
threshold	Specifies the upper temperature alarm threshold.	The value is an integer that ranges from 20 to 110, in °C.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the upper temperature alarm threshold for an AP. When an AP's temperature exceeds the upper threshold, the AP generates an alarm and a log, and notifies the AC of the high temperature alarm.

The parameter **ap-environment** is supported only by the AirEngine 9700D-M and AirEngine 9700D-M1. The parameters **cpu** and **np** are supported only by the AirEngine 9700D-M.

If **ap-environment** | **cpu** | **np** is not specified, this command sets an upper temperature alarm threshold for APs.

Example

Set the upper temperature alarm threshold for APs to 65°C.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] high-temperature threshold 65
```

11.2.114 ipsg enable (AP wired port profile view)

Function

The **ipsg enable** command enables IP source guard (IPSG) on an AP's wired interface.

The **undo ipsg enable** command disables IPSG on an AP's wired interface.

By default, IPSG is disabled on an AP's wired interface.

Format

ipsg enable

undo ipsg enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attackers often use packets with the source IP addresses or MAC addresses of authorized users to access or attack networks. As a result, authorized users cannot obtain stable and secure network services. You can enable the IPSG function to prevent the situation.

Prerequisites

Terminal address learning has been enabled on the AP's wired interface using the **learn-client-address enable** command.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

This command takes effect only on IP packets transmitted on an AP's wired interface.

An AP's wired interface added to an Eth-Trunk does not support this function.

Example

Enable IPSG on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] ipsg enable
```

11.2.115 ip-address (AP view)

Function

The **ip-address** command configures a static IPv4 address and gateway for an AP.

The **undo ip-address** command restores the default static IPv4 address and gateway for an AP.

By default, no static IPv4 address and gateway are configured for an AP.

Format

ip-address *ip-address* { *mask-length* | *mask* } [**gateway** *gateway*]

undo ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the static IPv4 address for an AP.	The value is in dotted decimal notation.
mask	Specifies the IPv4 address mask for an AP.	The value is in dotted decimal notation.
mask-length	Specifies the IPv4 address mask length for an AP.	The value is an integer that ranges from 0 to 32.
gateway *gateway*	Specifies the egress gateway for AP routes.	The value is in dotted decimal notation.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure an AP to go online using a specified IPv4 address, run the command to configure a static IPv4 address for the AP.

Prerequisites

The AP has been configured to obtain an IP address in static mode using the **address-mode (AP provisioning view)** command.

Precautions

Ensure that there are reachable routes between the configured IPv4 address and the AC source address for an AP to go online. Otherwise, the AP may fail to go online.

CAPWAP packets between the central AP and RUs in versions earlier than V200R019C10 are forwarded at Layer 2 and are independent of IP addresses on an agile distributed WLAN. Therefore, the configuration of an IP address does not affect the RU going online. Ensure that a route is reachable between the IP address of the RU and the central AP source address. Otherwise, services involving IP addresses may be affected, for example, STelnet.

If the AP and AC are connected through a Layer 3 network, the egress gateway for AP routes must be configured.

Example

Set the static IPv4 address of the AP to 10.1.1.1/24.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] address-mode static
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
[HUAWEI-wlan-ap-0] ip-address 10.1.1.1 24
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.116 ip-address (AP provisioning view)

Function

The **ip-address** command configures a static IPv4 address and gateway for an AP.

The **undo ip-address** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, no static IPv4 address and gateway are configured for an AP.

Format

ip-address *ip-address* { *mask-length* | *mask* } [**gateway** *gateway*]

undo ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the static IPv4 address for an AP.	The value is in dotted decimal notation.
mask	Specifies the IPv4 address mask for an AP.	The value is in dotted decimal notation.
mask-length	Specifies the IPv4 address mask length for an AP.	The value is an integer that ranges from 0 to 32.
gateway *gateway*	Specifies the egress gateway for AP routes.	The value is in dotted decimal notation.

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure an AP to go online using a specified IPv4 address, run the **ip-address** command to configure a static IPv4 address for the AP.

Prerequisites

The AP has been configured to obtain an IP address in static mode using the **address-mode (AP provisioning view)** command.

Follow-up Procedure

Run the **commit** command to deliver configuration to APs and restart the APs to make the configuration take effect.

Precautions

Ensure that there are reachable routes between the configured IPv4 address and the AC source address for an AP to go online. Otherwise, the AP may fail to go online.

CAPWAP packets between the central AP and RUs are forwarded at Layer 2 and are independent of IP addresses on an agile distributed WLAN. Therefore, the configuration of an IP address does not affect the RU going online. Ensure that a route is reachable between the IP address of the RU and the central AP source address. Otherwise, services involving IP addresses, for example, Telnet, may be affected.

If the AP and AC are connected through a Layer 3 network, the egress gateway for AP routes must be configured.

Example

Set the static IPv4 address of the AP to 10.1.1.1/24.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] address-mode static
[HUAWEI-wlan-provision-ap] ip-address 10.1.1.1 24
```

11.2.117 ip domain-name

Function

The **ip domain-name** command sets the default domain name suffix.

The **undo ip domain-name** command deletes the default domain name suffix.

By default, no default domain name suffix is provided.

Format

ip domain-name *domain-name*

undo ip domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name suffix.	The value is a string of 1 to 255 characters.

Views

AP view, AP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Devices with the same system name may exist in different domains. In this case, you can configure a fully qualified domain name (FQDN) for a device to uniquely identify it. The FQDN of a device consists of the default domain name suffix and device name. You can run the **ip domain-name** command to set the default domain name suffix and the **sysname** command to set the device name.

Precautions

If you run this command multiple times, the latest configuration overrides the previous ones.

Example

Set the domain name suffix to **com.cn**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] ip domain-name com.cn
```

11.2.118 igmp-snooping enable (AP wired port profile view)

Function

The **igmp-snooping enable** command enables IGMP snooping on an AP's wired interface.

The **undo igmp-snooping enable** command disables IGMP snooping on an AP's wired interface.

By default, IGMP snooping is disabled on an AP's wired interface.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP snooping is a basic Layer 2 multicast function that forwards and controls multicast traffic at the data link layer. IGMP snooping runs on a Layer 2 device and analyzes IGMP messages exchanged between a Layer 3 device and hosts to set up and maintain a Layer 2 multicast forwarding table. The Layer 2 device forwards multicast packets based on the Layer 2 multicast forwarding table.

Prerequisites

An AP wired port profile has been created.

Precautions

The AP wired interfaces added to an Eth-trunk interface do not support this function.

The **igmp-snooping enable** command is used to enable Layer 2 multicast services. To ensure multicast service experience, you are advised to disable the multicast packet rate limiting function by using the **traffic-optimize broadcast-suppression other-multicast disable** command in the AP system profile view.

When multicast services are enabled, the multicast services may be affected if rate limiting for multicast packets is enabled on an AP. In this case, you are advised to run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command to adjust the rate limit threshold for multicast packets.

Example

Enable IGMP snooping on AP wired port profile **p1**.

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



```
[HUAWEI-wlan-view] wired-port-profile name p1
[HUAWEI-wlan-wired-port-p1] igmp-snooping enable
```

11.2.119 keep-service enable

Function

The **keep-service enable** command enables service holding upon CAPWAP link disconnection.

The **undo keep-service enable** command disables service holding upon CAPWAP link disconnection.

By default, service holding upon CAPWAP link disconnection is disabled.

Format

keep-service enable

undo keep-service enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In direct forwarding mode, you can enable service holding upon CAPWAP link disconnection. In this way, when the CAPWAP link between an AP and AC is disconnected, the AP can continue to provide WLAN services, preventing service interruption and improving forwarding reliability.

Precautions

Service holding upon CAPWAP link disconnection can be configured in the VAP profile view and AP system profile view. The configuration in the VAP profile view takes precedence over that in the AP system profile view.

Service holding upon CAPWAP link disconnection is mutually exclusive with the containment function. Service holding upon CAPWAP link disconnection does not take effect when the containment function is also configured.

After service holding upon CAPWAP link disconnection is enabled, the **display access-user** command cannot display information about NAC STAs that are online before the CAPWAP link is disconnected. To display information about such STAs, run the **display station** command.

Example

Configure the AP to continue providing data services after the CAPWAP link between the AP and AC is disconnected.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] keep-service enable
```

11.2.120 keep-service enable allow new-access

Function

The **keep-service enable allow new-access** command enables offline APs to allow access of new STAs.

The **undo keep-service enable** command disables offline APs from allowing access of new STAs.

By default, offline APs cannot allow access of new STAs.

Format

keep-service enable allow new-access [**no-auth**]

undo keep-service enable

Parameters

Parameter	Description	Value
no-auth	Allows access of STAs using Portal or MAC address authentication.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Service holding upon CAPWAP link disconnection controls whether new STAs are allowed to go online. For high-security authentication modes such as MAC address authentication and Portal authentication, **no-auth** must be configured to enable STAs to go online without authentication upon CAPWAP link disconnection. Therefore, this function can be enabled in scenarios with low security requirements.

Precautions

The function of enabling offline APs to allow access of STAs is applicable to scenarios where service data is forwarded in direct mode and the STA authentication mode is Portal, MAC address, WEP, WPA/WPA2-PSK, or open system.

Example

Enable offline APs to allow access of new STAs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] keep-service enable allow new-access
```

11.2.121 learn-client-address enable (AP wired port profile view)

Function

The **learn-client-address enable** command enables STA address learning on an AP's wired interface.

The **undo learn-client-address enable** command disables STA address learning on an AP's wired interface.

By default, STA address learning is disabled on an AP's wired interface.

Format

learn-client-address { **ipv4** | **ipv6** } **enable**

undo learn-client-address { **ipv4** | **ipv6** } **enable**

Parameters

Parameter	Description	Value
ipv4	Indicates the IPv4 address.	-
ipv6	Indicates the IPv6 address.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After STA address learning is enabled on an AP's wired interface, if a wired terminal connected to the AP's wired interface successfully obtains an IP address, the AP automatically reports the IP address of the terminal to the AC, helping to maintain the ARP binding entries of wired terminals.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

An AP's wired interface added to an Eth-Trunk does not support this function.

STA address learning on an AP's wired interface takes effect only for STAs that obtain IP addresses through DHCP, and does not take effect for STAs using static IP addresses.

If a bridging device functions as a STA to connect to an AP enabled with STA address learning, the AP cannot learn IP addresses of users connected to the bridging device; therefore, the users cannot communicate with the network. In this situation, disable STA address learning.

Example

Enable STA IPv4 address learning on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] learn-client-address ipv4 enable
```

11.2.122 led blink-time

Function

The **led blink-time** command configures the indicator blinking function for an AP.

The **undo led blink-time** command cancels the indicator blinking configuration of an AP.

By default, the indicator blinking function is disabled on an AP.

Format

led blink-time *blink-time* { **ap-mac** *ap-mac* | **ap-name** *ap-name* | **ap-id** *ap-id* }

undo led blink-time { **ap-mac** *ap-mac* | **ap-name** *ap-name* | **ap-id** *ap-id* | **all** }

Parameters

Parameter	Description	Value
blink-time	Specifies the blinking time of an AP.	The value is an integer that ranges from 1 to 86400, in seconds.

Parameter	Description	Value
ap-mac *ap-mac*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.
all	Cancels the indicator blinking configuration of all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To locate an AP, run this command on the AC to configure the AP indicator to blink.

When this function is enabled, the SYS indicator blinks red.

Precautions

Offline APs cannot be located by configuring the AP indicator to blink.

The configuration using the **led blink-time** command takes precedence over that using the **led off** command. That is, if AP indicators are configured to blink and to turn off or turn off during the specified time range, the configuration performed using the **led off** command takes effect after the RU indicators blink.

This function is not available for central APs.

Example

Configure the indicator of an AP with the MAC address of 00e0-fc12-3456 to blink for 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] led blink-time 300 ap-mac 00e0-fc12-3456
```


11.2.123 led off

Function

The **led off** command turns off AP indicators.

The **undo led off** command restores the default settings.

By default, AP indicators are allowed to turn on.

Format

led off

undo led off

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Blinking indicators of indoor APs deployed in hospitals and hotels may affect people's nighttime rest. To prevent this, run the **led off** command to turn off AP indicators.

If you need to locate AP faults by observing AP indicator status, run the **undo led off** command to allow the AP indicators to turn on.

Precautions

The configuration performed using the **led blink-time** command takes precedence over that performed using the **led off** command. That is, if AP indicators are configured to blink and to turn off or turn off during the specified time range, the configuration performed using the **led off** command takes effect after the RU indicators blink.

Example

Turn off AP indicators.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] led off
```


11.2.124 lldp admin-status

Function

The **lldp admin-status** command sets the LLDP operation mode for an AP.

The **undo lldp admin-status** command restores the default LLDP operation mode for an AP.

By default, the LLDP operation mode of an AP is TxRx.

Format

lldp admin-status { **rx** | **tx** | **txrx** }

undo lldp admin-status

Parameters

Parameter	Description	Value
rx	Specifies the LLDP operation mode as Rx. An AP only receives but does not send LLDP packets.	-
tx	Specifies the LLDP operation mode as Tx. An AP only sends but does not receive LLDP packets.	-
txrx	Specifies the LLDP operation mode as TxRx. An AP sends and receives LLDP packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can configure the LLDP operation mode for an AP based on the site requirements. For example, if you set the LLDP operation mode of an AP to Tx, the AP sends LLDP packets but cannot receive LLDP packets from neighbors. In this situation, the AP cannot discover neighbors.

Example

Set the LLDP operation mode of an AP to Tx.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp admin-status tx
```

11.2.125 lldp dot3-tlv power (AP wired port link profile view)

Function

The **lldp dot3-tlv power** command configures the standard with which the 802.3 Power via MDI TLV advertised by an AP's wired interface complies.

By default, the 802.3 Power via MDI TLV advertised by a UPoE interface and a PoE interface complies with 802.3bt and 802.3at, respectively.

Format

lldp dot3-tlv power { **802.1ab** | **802.3at** | **802.3bt** }

undo lldp dot3-tlv power

Parameters

Parameter	Description	Value
802.1ab	Indicates that the 802.3 Power via MDI TLV advertised an AP's wired interface complies with 802.1ab.	-
802.3at	Indicates that the 802.3 Power via MDI TLV advertised an AP's wired interface complies with 802.3at.	-
802.3bt	Indicates that the 802.3 Power via MDI TLV advertised an AP's wired interface complies with 802.3bt.	-

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.3 Power via MDI TLV advertised by an AP's wired interface supports the following formats:

- 802.1ab format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class]
- 802.3at format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value]
- 802.3bt format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value | PD requested power value Mode A | PD requested power value Mode B | PSE allocated power value Alternative A | PSE allocated power value Alternative B | PSE power status | System setup | PSE maximum available power | Autoclass | Power down]

Based on 802.1ab, 802.3at extends three fields: type/source/priority, PD requested power value, and PSE allocated power value. Based on 802.3at, 802.3bt extends the following fields to provide more detailed UPoE information: PD requested power value Mode A, PD requested power value Mode B, PSE allocated power value Alternative A, PSE allocated power value Alternative B, PSE power status, System setup, PSE maximum available power, Autoclass, and Power down.

Prerequisites

- The LLDP function has been enabled in both the WLAN view and AP wired port link profile view.
- APs' wired interfaces are allowed to advertise the 802.3 Power via MDI TLV.

Precautions

Before selecting a format of the 802.3 Power via MDI TLV, you need to know the TLV formats supported by the neighbors. The TLV format on the local device must be the same as that on the neighbors.

Member interfaces of the Eth-Trunk do not support this command.

Example

Configure the 802.3 Power via MDI TLV advertised by the AP's wired interface to comply with 802.3at.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp dot3-tlv power 802.3at
```

11.2.126 lldp enable

Function

The **lldp enable** command enables LLDP on an AP's wired interface.

The **undo lldp enable** command disables LLDP on an AP's wired interface.

By default, LLDP is enabled on an AP's wired interface.

Format

lldp enable

undo lldp enable

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AP wired interfaces can exchange LLDP packets with neighbors to obtain neighbor status and transmit AP status to neighbors. The AP and neighbors save the received information to the Management Information Base (MIB) to query and determine the link status.

Prerequisite

The LLDP function has been enabled in the WLAN view using the **ap lldp enable** command.

Example

Enable LLDP on the AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap lldp enable
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp enable
```

11.2.127 lldp message-transmission delay (AP system profile view)

Function

The **lldp message-transmission delay** command sets the LLDP packet transmission delay.

The **undo lldp message-transmission delay** command restores the default LLDP packet transmission delay.

The default LLDP packet transmission delay is 2 seconds.

Format

lldp message-transmission delay *delay*

undo lldp message-transmission delay

Parameters

Parameter	Description	Value
delay	Specifies the LLDP packet transmission delay.	The value is an integer that ranges from 1 to 8192, in seconds. The *delay* value depends on the parameter *interval* set by the **lldp message-transmission interval** command. The *delay* value must be less than or equal to a quarter of the *interval* value.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before the AP sends an LLDP packet to the neighbor when the device status changes frequently.

If the AP status changes frequently, extend the delay in preventing the AP from frequently sending packets to the neighbors. A delay suppresses the network topology flapping.

Configuration Impact

The LLDP packet transmission delay must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency when the local device status frequently changes. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.

- A small value increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time when the local device status frequently changes. However, if the value is too small, LLDP packets are exchanged frequently. This increases the system load and wastes resources.
- The default value is recommended.

Precautions

Consider the value of *interval* when adjusting the value of *delay* because it is restricted by the value of *interval*.

- Decreasing the value of *delay* is not restricted by the value of *interval*. *delay* can be any number from 1 to 8192.
- The *delay* value must be less than or equal to a quarter of the *interval* value. Therefore, if you want to set *delay* to be greater than a quarter of *interval*, first increase the *interval* value to at least four times the new *delay* value, and then increase the *delay* value.

NOTE

If the *interval* value is smaller than four times the *delay* value, the system displays an error message when you run the **undo lldp message-transmission delay** command. To run the **undo lldp message-transmission delay** command, increase the *interval* value to at least four times the *delay* value first.

Example

Set the LLDP packet transmission delay to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp message-transmission delay 10
```

11.2.128 lldp message-transmission hold-multiplier (AP system profile view)

Function

The **lldp message-transmission hold-multiplier** command sets the hold time multiplier of device information stored on neighbors.

The **undo lldp message-transmission hold-multiplier** command restores the default hold time multiplier of device information stored on neighbors.

The default hold time multiplier is 4.

Format

lldp message-transmission hold-multiplier *hold*

undo lldp message-transmission hold-multiplier

Parameters

Parameter	Description	Value
hold	Specifies the hold time multiplier of device information stored on neighbors.	The value is an integer that ranges from 2 to 10.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The time multiplier is used to calculate how long a packet can be saved on a neighboring node. After receiving an LLDP packet, a neighbor updates the aging time of the device information from the sender based on the TTL.

The storage time calculation formula is: TTL = Min (65535, (*interval* x *hold*)).

TTL is the device information storage time. It is the smaller value between 65535 and (*interval* x *hold*).

interval indicates the interval at which the device sends LLDP packets to neighbors. This parameter is set by the **lldp message-transmission interval** command. *hold* indicates the hold time multiplier of device information stored on neighbors.

After the LLDP function is disabled on the device, its neighbors wait until the TTL of the device information expires, and then delete the device information. This prevents network topology flapping.

Configuration Impact

The hold time multiplier of device information stored on neighbors must be set to a proper value.

- A large value of *delay* prevents network topology flapping. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value of *delay* enables the NMS to discover topology change in time. However, if the value is too small, the neighbors update device information too frequently. This increases the load on the system and wastes resources.
- The default value is recommended.

Example

Set the hold time multiplier of AP information stored on neighbors to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp message-transmission hold-multiplier 5
```

11.2.129 lldp message-transmission interval (AP system profile view)

Function

The **lldp message-transmission interval** command sets the LLDP packet transmission interval.

The **undo lldp message-transmission interval** command restores the default LLDP packet transmission interval.

The default LLDP packet transmission interval is 30 seconds.

Format

lldp message-transmission interval *interval*

undo lldp message-transmission interval

Parameters

Parameter	Description	Value
interval	Specifies the LLDP packet transmission interval.	The value is an integer that ranges from 5 to 32768, in seconds. The *interval* value depends on the parameter *delay* set by the **lldp message-transmission delay** command. The *interval* value must be greater than or equal to 4 times the *delay* value; otherwise, the system displays an error message when you run the **lldp message-transmission interval** command.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the LLDP status of the AP keeps unchanged or the AP does not discover new neighbors, the AP sends LLDP packets to the neighbors at a specified interval.

If you want to change the network topology detection frequency, run the **lldp message-transmission interval** command to change the LLDP packet transmission interval.

Configuration Impact

The LLDP transmission interval must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A short interval increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time. If the delay is too short, LLDP packets are exchanged frequently. This increases the system load and wastes resources.
- The default value is recommended.

Precautions

Consider the value of *delay* when adjusting the value of *interval* because it is restricted by the value of *interval*.

- Increasing the value of *interval* is not restricted by the value of *delay*. *interval* can be any number from 5 to 32768.
- The *interval* value must be greater than or equal to four times the *delay* value. Therefore, if you want to set *interval* to be smaller than four times the value of *delay*, first reduce the *delay* value to be less than or equal to a quarter of the new *interval* value, and then reduce the *interval* value.

NOTE

If the *delay* value is larger than a quarter of the *interval* value, the system displays an error message when you run the **undo lldp message-transmission interval** command. To run the **undo lldp message-transmission interval** command, reduce the *delay* value to be less than or equal to a quarter of the *interval* value first.

Example

Set the LLDP packet transmission interval to 60 seconds.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp message-transmission interval 60
```

11.2.130 lldp report enable

Function

The **lldp report enable** command enables an AP to report information about its LLDP neighbors.

The **undo lldp report enable** command disables an AP from reporting information about its LLDP neighbors.

By default, an AP does not report information about its LLDP neighbors.

Format

lldp report enable

undo lldp report enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **lldp report enable** command to enable an AP to report information about its LLDP neighbors.

Example

Enable an AP to report information about its LLDP neighbors.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] lldp report enable
```


11.2.131 lldp report-interval

Function

The **lldp report-interval** command sets the interval at which an AP reports LLDP neighbor information.

The **undo lldp report-interval** command restores the default interval at which an AP reports LLDP neighbor information.

By default, an AP reports LLDP neighbor information at an interval of 30 seconds.

Format

lldp report-interval *interval-time*

undo lldp report-interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval at which an AP reports LLDP neighbor information to an AC.	The value is an integer that ranges from 5 to 3600, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **lldp report-interval** command to adjust the interval at which an AP reports LLDP neighbor information. This prevents LLDP neighbor information from being frequently reported.

Example

Set the interval at which an AP reports LLDP neighbor information to an AC to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp report-interval 20
```


11.2.132 lldp restart-delay

Function

The **lldp restart-delay** command sets the delay in re-enabling LLDP on an AP.

The **undo lldp restart-delay** command restores the default delay in re-enabling the LLDP function on an AP.

By default, the delay in re-enabling LLDP on an AP is 2 seconds.

Format

lldp restart-delay *delay-time*

undo lldp restart-delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay in re-enabling LLDP.	The value is an integer that ranges from 1 to 10, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When the LLDP status of an AP changes, the AP reports LLDP neighbor information. Setting the delay in re-enabling LLDP on the AP prevents the AP from frequently reporting LLDP neighboring information when the LLDP status of the AP frequently changes.

Example

Set the delay in re-enabling LLDP on an AP to 1 second.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp restart-delay 1
```


11.2.133 lldp tlv-enable (AP wired port link profile view)

Function

The **lldp tlv-enable** command specifies the types of TLVs that an AP wired interface advertises.

The **undo lldp tlv-enable** command specifies the types of TLVs that an AP wired interface is prohibited from advertising.

By default, an AP wired interface advertises all types of TLVs.

Format

lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

lldp tlv-enable dot3-tlv power

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp tlv-enable dot3-tlv power

Parameters

Parameter	Description	Value
basic-tlv	Indicates basic TLVs to be advertised: ● Management-address TLV ● Port Description TLV ● System Capabilities TLV ● System Description TLV ● System Name TLV	-
all	Configures the AP wired interface to advertise all types of TLVs when basic TLVs are configured.	-
management-address	Configures the AP wired interface to advertise Management-address TLVs.	-
port-description	Configures the AP wired interface to advertise Port Description TLVs.	-
system-capability	Configures the AP wired interface to advertise System Capabilities TLVs.	-
system-description	Configures the AP wired interface to advertise System Description TLVs.	-
system-name	Configures the AP wired interface to advertise System Name TLVs.	-

Parameter	Description	Value
dot3-tlv	Configures an AP's wired interface to advertise TLVs defined by IEEE 802.3.	-
power	Configures an AP's wired interface to advertise the Power Via MDI TLV defined by IEEE 802.3 and negotiate the PoE power.	-

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent.

Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. The TLVs that can be encapsulated in an LLDP packet include basic TLVs and TLVs in the IEEE 802.3 format.

Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.3 format are defined by standardization organizations and other organizations, which are used to enhance the network device management. You can determine whether to advertise the TLVs in the IEEE 802.3 format.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

Prerequisites

The LLDP function has been enabled in both the WLAN view and AP wired port link profile view.

Precautions

When basic TLVs are configured, if the **all** parameter is specified, all optional basic TLVs are advertised. If the **all** parameter is not specified, TLVs of only one type can be advertised at a time. To advertise multiple types of TLVs, run this command multiple times.

Example

Configure the wired interface of AP to advertise Management-address TLVs.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap lldp enable
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp tlv-enable basic-tlv management-address
```

11.2.134 lldp tlv-enable legacy-tlv four-pair-power (AP wired port link profile view)

Function

The **lldp tlv-enable legacy-tlv four-pair-power** command configures an AP's wired interface to advertise Cisco's customized TLVs.

The **undo lldp tlv-enable legacy-tlv four-pair-power** command prohibits an AP's wired interface from advertising Cisco's customized TLVs.

By default, an AP's wired interface advertises Cisco's customized TLVs.

Format

lldp tlv-enable legacy-tlv four-pair-power

undo lldp tlv-enable legacy-tlv four-pair-power

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some Cisco's switches use customized LLDP TLVs to negotiate the UPoE power supply. If such a switch is used to supply UPoE power to an AP, the AP's wired interface connected to the switch must be enabled to advertise Cisco's customized TLVs for UPoE power negotiation. Otherwise, LLDP negotiation fails. If interfaces on the Cisco's switch do not supply UPoE power, the AP is provided with insufficient input power and cannot work properly.

Example

Configure an AP's wired interface to advertise Cisco's customized TLVs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp tlv-enable legacy-tlv four-pair-power
```


11.2.135 lldp tlv-enable legacy-tlv power-capability (AP wired port link profile view)

Function

The **lldp tlv-enable legacy-tlv power-capability** command configures LLDP packets sent by an AP to carry the supported power capability.

The **undo lldp tlv-enable legacy-tlv power-capability** command configures LLDP packets sent by an AP not to carry the supported power capability.

By default, the LLDP packets sent by an AP carry the supported power capability.

Format

lldp tlv-enable legacy-tlv power-capability

undo lldp tlv-enable legacy-tlv power-capability

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When directly connected to a Huawei PoE switch, the AP can send its power capability to the switch through LLDP. If the total output power of the PoE switch exceeds the threshold, the switch adjusts the output power of the corresponding Ethernet port based on the power capability of the AP. This reduces the output power without affecting the basic functions of the AP.

Example

Configure the LLDP packets sent by an AP to carry the supported power capability.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp tlv-enable legacy-tlv power-capability
```


11.2.136 location

Function

The **location** command configures the installation position of an AP.

The **undo location** command deletes the installation position of an AP.

By default, an AP's installation position is not configured.

NOTE

This command is not available for the following APs:

- AirEngine 5761-10W and AirEngine 5761S-10W

Format

location *location-value*

undo location

Parameters

Parameter	Description	Value
location-value	Specifies the installation position of an AP.	The value is a string of 1 to 63 case-sensitive characters. If the value contains space, it must start and end with double quotation marks ("), for example, **"hello name1"**. Each double quotation mark in the value occupies one character. The value cannot start or end with spaces and double quotation marks ("). For example, **" HELLO"** and **"HELLO "** are not allowed.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the installation position of an AP.

Example

Configure the installation position of an AP to **B2-5F-01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] location B2-5F-01
```

11.2.137 log-record-level

Function

The **log-record-level** command configures the level for AP logs that need to be backed up.

The **undo log-record-level** command restores the default level of AP logs that need to be backed up.

By default, the level of AP logs that need to be backed up is **info**.

Format

log-record-level { **alert** | **critical** | **debug** | **emergency** | **error** | **info** | **notice** | **warning** }

undo log-record-level

Parameters

Parameter	Description	Value
alert	Configures the level of logs as **alert**, that is, the AP backs up logs that need to be processed immediately.	-
critical	Configures the level of logs as **critical**, that is, the AP backs up critical logs.	-
debug	Configures the level of logs as **debug**, that is, the AP backs up debugging logs.	-
emergency	Configures the level of logs as **emergency**, that is, the AP backs up unavailable logs.	-
error	Configures the level of logs as **error**, that is, the AP backs up error logs.	-
info	Configures the level of logs as **info**, that is, the AP backs up normal logs.	-
notice	Configures the level of the logs as **notice**, that is, the AP backs up logs that need to be noticed.	-

Parameter	Description	Value
warning	Configures the level of logs as **warning**, that is, the AP backs up warning logs.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP periodically backs up logs to the log server. However, not all the logs need to be backed up. You can run the **log-record-level** command to configure the level of logs to be periodically backed up.

Precautions

The preference order of log levels is emergency, alert, critical, error, warning, notice, info, and debug.

After you specify the level for AP logs that need to be backed up, all logs of the specified level or a higher level will be backed up. For example, if you set the level of AP logs that need to be backed up to **critical**, the logs of the levels **emergency**, **alert**, and **critical** will be backed up.

Example

Set the level of logs that need to be backed up as **alert**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] log-record-level alert
```

11.2.138 log-server

Function

The **log-server** command configures the log server IP address and port number in the AP system profile and enables log backup on the AP.

The **undo log-server** command restores the default log server IP address and port number in the AP system profile and disables log backup on the AP.

By default, the port number of the log server is 514 in UDP mode, the log server IP address is not configured in an AP system profile, and log backup is disabled on an AP.

Format

log-server ip-address *server-ip-address* [**port** *port*]

undo log-server

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies the IPv4 address of the log server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of the log server.	The value is an integer that ranges from 1 to 65535. The default port number is 514.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **log-server** command to configure the log server IP address and port number in the AP system profile and enable log backup on the AP. After log backup is enabled, the AP automatically sends logs to the log server with the specified IP address.

NOTICE

Modifying the configuration of an AP system profile changes configurations of all APs using this profile.

Example

Set the IP address of the log server to 10.0.0.1 and port number to 2000 and enable log backup on the AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] log-server ip-address 10.0.0.1 port 2000
```


11.2.139 low-temperature threshold

Function

The **low-temperature threshold** command sets a lower device, ambient, CPU, or NP module temperature alarm threshold for APs.

The **undo low-temperature threshold** command restores the default lower device, ambient, CPU, or NP module temperature alarm threshold of APs.

Table 11-127 Default lower temperature alarm threshold for APs

AP Model	Default Value (°C)
/AirEngine 9700D-M1 (AP device and environment)	-3

NOTE

This command is not supported by the following models:

- AirEngine series APs

Format

low-temperature [**ap-environment** | **cpu** | **np**] **threshold** *threshold*

undo low-temperature [**ap-environment** | **cpu** | **np**] **threshold**

Parameters

Parameter	Description	Value
ap-environment	Indicates the ambient temperature.	-
cpu	Indicates the CPU temperature.	-
np	Indicates the NP module temperature.	-
threshold	Specifies the lower temperature alarm threshold.	The value is an integer that ranges from -70 to +10, in °C.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the lower temperature alarm threshold for an AP. When an AP's temperature exceeds the lower threshold, the AP generates an alarm and a log, and notifies the AC of the low temperature alarm.

The parameter **ap-environment** is supported only by the AirEngine 9700D-M and AirEngine 9700D-M1. The parameters **cpu** and **np** are supported only by the AirEngine 9700D-M.

If **ap-environment** | **cpu** | **np** is not specified, this command sets a lower temperature alarm threshold for APs.

Example

Set the lower temperature alarm threshold for APs to 5°C.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] low-temperature threshold 5
```

11.2.140 mac-learning (AP wired port profile view)

Function

The **mac-learning** command configures the MAC address learning priority and packet forwarding policy of an AP's wired interface.

The **undo mac-learning** command restores the default MAC address learning priority and packet forwarding policy of an AP's wired interface.

By default, the MAC address learning priority of an AP's wired interface is 0 and the packet forwarding policy is forward.

Format

mac-learning { **priority** *priority* | **action discard** } *

undo mac-learning priority

undo mac-learning action

Parameters

Parameter	Description	Value
priority *priority*	Specifies the MAC address learning priority of an AP's wired interface.	The value is an integer that ranges from 0 to 3. A larger value indicates a higher priority.
action discard	Configures an AP's wired interface to discard the packet if a wired interface with a higher MAC address learning priority has learned the same MAC address as that carried in this packet.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP with multiple network interfaces connects to the upper-layer network through its uplink interfaces and provides access to STAs through its downlink interfaces. If the interfaces with different MAC address learning priorities learn the same MAC address, the MAC address entry learned by the interface with the highest priority overrides those learned by other interfaces, but not vice versa.

When an interface with a lower MAC address learning priority receives a packet carrying the MAC address learned by an interface with a higher priority, the local interface can be configured to discard or forward the packet.

Example

Set the MAC address learning priority to 1 in an AP wired port profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mac-learning priority 1
```


11.2.141 management-vlan (AP system profile view, AP provisioning view, AP view)

Function

The **management-vlan** command configures CAPWAP packets sent from an AP's wired interface to carry a management VLAN tag.

The **undo management-vlan** command configures CAPWAP packets sent from an AP's wired interface not to carry a management VLAN tag.

In the AP system profile view and AP view, the **undo management-vlan** command configures CAPWAP packets sent from an AP's wired interface not to carry a management VLAN tag. In the AP provisioning view, the **undo management-vlan** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, CAPWAP packets sent from an AP's wired interface do not carry a management VLAN tag.

Format

management-vlan *vlan-id*

undo management-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of the management VLAN tag carried in CAPWAP packets sent from an AP's wired interface.	The value is an integer that ranges from 1 to 4094.

Views

AP system profile view, AP provisioning view, AP view

Default Level

2: Configuration level

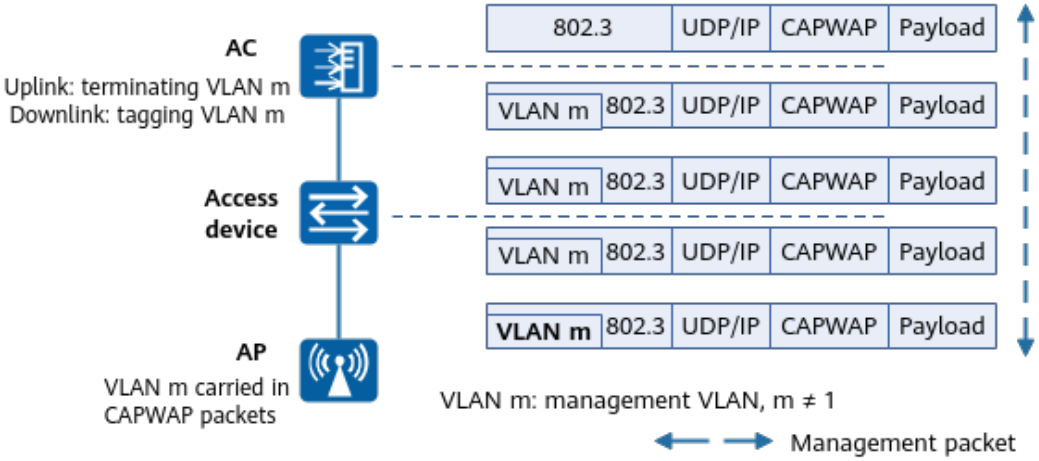
Usage Guidelines

Usage Scenario

By default, CAPWAP packets sent from an AP's wired interface do not carry a management VLAN tag. In most cases, the access switch interface directly connected to the AP adds the tag of the PVID to the CAPWAP packets as the management VLAN ID.

If the access device (for example, an unmanaged switch) does not support the VLAN function or the PVID of the device has been used for other purposes (for example, as the default VLAN ID of wired users), the access device cannot add the management VLAN tag to packets on the interface directly connected to the AP. In this case, you can configure CAPWAP packets sent by an AP's wired interface to carry the management VLAN tag so that the AP adds the management VLAN tag to the CAPWAP packets before sending them to the AC.

Figure 11-1 Flowchart for configuring CAPWAP packets sent by an AP's wired interface to carry the management VLAN tag



Precautions

This configuration takes effect only after the APs restart if the **management-vlan** command is configured in the AP system profile view or AP view.

If the **management-vlan** command is configured in the AP provisioning view, run the **commit** command to deliver the configuration. The configuration takes effect after the APs restart.

On a Mesh network, ensure that CAPWAP packets sent from all APs carry the same management VLAN. Otherwise, Mesh Points (MPs) cannot go online.

Based on the access device capability and PVID configuration, the requirements for configuring CAPWAP packets sent by an AP to carry the management VLAN tag are described in the following table.

Table 11-128 Requirements for configuring CAPWAP packets to carry the management VLAN tag

Access Device Capability and PVID Configuration	AP Configuration Requirements
The access device does not support the VLAN function.	CAPWAP packets are enabled to carry the management VLAN tag. Additionally, ensure that the AP's uplink wired interface is added to the management VLAN in tagged mode. By default, an AP's uplink wired interface joins all VLANs except VLAN 1 in tagged

Access Device Capability and PVID Configuration	AP Configuration Requirements
The access device supports the VLAN function, and the PVID of the interface directly connected to the AP is different from the management VLAN ID.	mode. Therefore, no additional configuration is required. To modify the configuration, run the **vlan tagged** *vlan-id* command in the AP wired port profile view and bind the profile to an AP or AP group.
The access device supports the VLAN function, and the PVID of the interface directly connected to the AP is the same as the management VLAN ID.	CAPWAP packets sent by an AP do not carry the management VLAN tag. The access device adds the management VLAN tag to CAPWAP packets. **NOTE** In this case, to enable CAPWAP packets to carry the management VLAN tag, run the **vlan pvid** *vlan-id* command to configure the PVID of the AP's uplink wired interface to be the same as the management VLAN ID. Otherwise, the AP cannot receive management packets, causing repeated disconnection and restart.

After the **management-vlan** *vlan-id* command is executed to configure AP's wired interfaces to send CAPWAP packets carrying the management VLAN tag (not VLAN 1), the interfaces working in **root** mode are added to VLAN 1 in tagged mode, which cannot be changed.

Example

Configure CAPWAP packets sent from an AP's wired interface to carry management VLAN 2 in the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] management-vlan 2
Warning: The incorrect management VLAN configuration will cause the AP to go out of management. This operation will make the AP reset. Continue? [Y/N]:y
```

Configure CAPWAP packets sent from a wired interface on AP 0 to carry management VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] management-vlan 2
Warning: The incorrect configuration will cause the AP to go out of management. This operation will deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
```

Configure CAPWAP packets sent from an AP's wired interface to carry management VLAN 2 in the AP provisioning view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] management-vlan 2
Warning: The incorrect management VLAN configuration will cause the AP to go out of management.
```



```
When the configuration is committed,
 the AP will reset.Continue?[Y/N]:y
```

11.2.142 memory-usage threshold

Function

The **memory-usage threshold** command configures a memory usage alarm threshold for APs.

The **undo memory-usage threshold** command restores the default memory usage alarm threshold.

By default, the memory usage alarm threshold on an AP is 80.

Format

memory-usage threshold *threshold*

undo memory-usage threshold

Parameters

Parameter	Description	Value
threshold	Specifies the memory usage alarm threshold of an AP.	The value is an integer that ranges from 30 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **memory-usage threshold** command to configure the memory usage alarm threshold in the AP system profile view. The configuration is delivered to all APs using the profile.

- When the memory usage of an AP exceeds the alarm threshold, .
- When the memory usage of an AP falls below the alarm threshold, .

Example

Set the memory usage alarm threshold of AP 0 to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] memory-usage threshold 60
```


11.2.143 mld-snooping enable (AP wired port profile view)

Function

The **mld-snooping enable** command enables MLD snooping on an AP's wired interface.

The **undo mld-snooping enable** command disables MLD snooping on an AP's wired interface.

By default, MLD snooping is disabled on an AP's wired interface.

Format

mld-snooping enable

undo mld-snooping enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MLD snooping is a basic IPv6 Layer 2 multicast function that forwards and controls multicast traffic at the data link layer. MLD snooping runs on a Layer 2 device and analyzes MLD messages exchanged between a Layer 3 device and hosts to set up and maintain a Layer 2 multicast forwarding table. The Layer 2 device forwards multicast packets based on the Layer 2 multicast forwarding table.

Prerequisites

An AP wired port profile has been created.

Precautions

The AP wired interfaces added to an Eth-trunk interface do not support this function.

Example

Enable MLD snooping on AP wired port profile **p1**.

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



```
[HUAWEI-wlan-view] wired-port-profile name p1
[HUAWEI-wlan-wired-port-p1] mld-snooping enable
```

11.2.144 mode (AP wired port profile view)

Function

The **mode** command sets the working mode for an AP's wired interface.

The **undo mode** command restores the default working mode of an AP's wired interface.

By default, the working modes of APs' wired interfaces vary depending on the AP models.

Table 11-129 Working modes of APs' wired interfaces

AP Model	root	endpoint	middle
AirEngine series indoor settled APs	All interfaces (including Eth-Trunk interfaces)	-	-
AirEngine series outdoor APs	All interfaces (including Eth-Trunk interfaces)	-	-
AirEngine series wall plate APs and RUs	Uplink port	Downlink port	-
AirEngine series central APs	Uplink port	-	Downlink port
AirEngine 9700D-S	GE port	-	-

NOTE

The working modes of wired interfaces cannot be changed on the following models:

Format

mode { **root** | **endpoint** | **middle** }

undo mode

Parameters

Parameter	Description	Value
root	Sets the working mode of an AP's wired interface to root, which can connect to an AC.	-
endpoint	Sets the working mode of an AP's wired interface to endpoint, which can connect to a host.	-
middle	Sets the working mode of an AP's wired interface to middle, which allows a central AP to connect to an RU.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When working as an uplink interface to connect to an AC, an AP's wired interface must work in root mode. In root mode, the AP's wired interface automatically joins service VLANs and user-specific VLANs (for example, VLANs assigned by the RADIUS server).

When working as a downlink interface to connect to a wired terminal, the AP's wired interface must work in endpoint mode. In endpoint mode, the AP's wired interface does not join any VLAN by default.

When the central AP connects to RUs through downlink GE interfaces, the working mode of the downlink GE interfaces must be set to **middle**.

Precautions

When the AP's wired interface works in root mode, user isolation cannot be configured. User isolation can be configured on an AP's wired interface only when the interface works in endpoint or middle mode.

When the AP's wired interface works in root mode and has been configured to transmit packets carrying the management VLAN tag using the **management-vlan** *vlan-id* command, the PVID for the AP's wired interface must be configured

the same as the management VLAN ID. If the AP's wired interface works in endpoint mode, the PVID can be configured directly. If the AP's wired interface works in middle mode, the PVID cannot be configured.

The configuration of the AP's wired interface takes effect after the AP is restarted.

Example

Set the working mode of the AP's wired interface ETH0 to **endpoint**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode configuration will cause the AP to go out of management . This fault can be recovered only by modifying the configuration on the AP.
Continue? [Y/N]:y
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired ethernet 0
```

11.2.145 mtu

Function

The **mtu** command sets the maximum transmission unit (MTU) value for the management VLANIF and CAPWAP on an AP.

The **undo mtu** command restores the default MTU value for the management VLANIF and CAPWAP on an AP.

By default, the MTU value of the management VLANIF and CAPWAP on an AP is 1500 bytes.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the maximum size of packets sent and received on the management VLANIF and CAPWAP.	The value is an integer that ranges from 1000 to 1700, in bytes.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MTU determines the maximum number of bytes in IP packets each time a sender can send. The MTU of an IP packet refers to the number of bytes from the IP header of the packet to the data.

The MTU in the AP system profile view is the maximum size of packets sent and received on the management VLANIF and CAPWAP of an AP.

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet to be sent, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than or equal to the MTU. If unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. To ensure jumbo packets are not dropped during transmission, you need to configure forcible fragmentation. In this case, you can run the **mtu** command to set the size of a fragment.

Therefore, a proper MTU is a prerequisite for normal communication on a network.

- If the configured MTU is excessively small and the packet size is larger, packets are discarded when being forwarded through the forwarding chip; packets are broken into a great number of fragments when being forwarded through the CPU, affecting proper data transmission.
- If the size of packets exceeds the MTU supported by a transit node or a receiver, the transit node or receiver fragments the packets or even discards them, aggravating the network transmission load.

The default MTU is recommended. When the size of packets to be transmitted or the device that receives packets changes, you can change the MTU based on the actual network.

Precautions

- DHCP packets cannot be fragmented. When the MTU value set using the **mtu** command is smaller than the DHCP packet length, DHCP packets cannot be forwarded. Therefore, set a larger MTU value.
- If the MTU value is smaller than the DHCP packet length, the AP may be disconnected. In this case, restart the AP.
- When the MTU is too small and the DF bit is set to 1, packets cannot be fragmented. In this case, use the forced fragmentation function.

Example

Set the MTU value of the management VLANIF and CAPWAP on an AP to 1700 bytes.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] mtu 1700
```

11.2.146 multicast-rate

Function

The **multicast-rate** command configures the multicast rate of wireless packets in a radio profile.

The **undo multicast-rate** command restores the default multicast rate of wireless packets in a radio profile.

By default, the multicast rate of wireless packets is not configured in a radio profile. That is, the multicast rate is set to auto-sensing.

Format

multicast-rate *multicast-rate*

undo multicast-rate

Parameters

Parameter	Description	Value
multicast-rate	Specifies the multicast rate of wireless packets in a radio profile.	The value is of the enumerated type: The values are as follows in a 2G radio profile: • 1: 1 Mbit/s • 2: 2 Mbit/s • 5: 5.5 Mbit/s • 6: 6 Mbit/s • 9: 9 Mbit/s • 11: 11 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s The values are as follows in a 5G radio profile: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After this command is run, the multicast rate of wireless packets is the configured value and irrelevant to the STA access mode.

If the configured multicast rate is not in the basic rate set and the STA does not support this rate, the STA cannot receive multicast data.

If you run the **radio-type dot11b** command in the 2G radio profile view to set the radio type to **dot11b**, and the 2G radio profile is applied to an AP, *multicast-rate* that takes effect on the 2 GHz radio of the AP is fixed as 1 Mbit/s, and *multicast-rate* configured in the 2G radio profile view does not take effect on the AP.

Example

Set the multicast rate of wireless packets to 54 Mbit/s in the 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] multicast-rate 54
```

11.2.147 multicast-suppression auto-detect (AP system profile view)

Function

The **multicast-suppression auto-detect** command configures the rate limit for multicast packets during intelligent flow control.

The **undo multicast-suppression auto-detect** command restores the default rate limit for multicast packets during intelligent flow control.

By default, the rate limit for multicast packets is 256 pps.

NOTE

This function is not supported by the following models:

- AirEngine X760 series APs (excluding the AirEngine 5760-10)
- AirEngine 9700D-S (including matching ORUs)

Format

multicast-suppression auto-detect packets *packets*

undo multicast-suppression auto-detect

Parameters

Parameter	Description	Value
packets *packets*	Specifies the rate limit for multicast packets.	The value is an integer that ranges from 64 to 1024, in pps.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When there are a large number of broadcast, multicast, and unknown unicast packets, the CPU becomes busy processing these packets and the buffer of the packet for receiving incoming packets is occupied. When the buffer decreases to the specified threshold, the device automatically rate-limits the broadcast, multicast, and unknown unicast packets. You can run this command to specify the rate limit for intelligent flow control as required. Rate limiting takes effect only for incoming traffic.

Example

Set the rate limit for multicast packets during intelligent flow control to 300 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] multicast-suppression auto-detect packets 300
```

11.2.148 np capwap-reassembly (AP system profile view)

Function

The **np capwap-reassembly disable** command disables the NP CAPWAP reassembly function of the AP.

The **undo np capwap-reassembly disable** command restores the default status of the NP CAPWAP reassembly function of APs.

By default, the NP CAPWAP reassembly function operates in adaptive mode for APs. That is, this function is enabled when services run properly, and is automatically disabled upon an exception.

NOTE

NP CAPWAP reassembly is supported only by AirEngine X760 series APs and AirEngine 9700D-S (including matching ORUs).

Format

np capwap-reassembly disable

undo np capwap-reassembly disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the NP CAPWAP reassembly function, the NP replaces the CPU to reassemble the received CAPWAP fragments. This speeds up the packet processing and improves the forwarding performance.

Precautions

If the **np fast-forwarding disable** command has been run, the NP CAPWAP reassembly function of the AP is also disabled. To enable NP CAPWAP reassembly of the AP, run the **undo np fast-forwarding disable** and **undo np capwap-reassembly disable** commands in sequence.

Example

Disable the NP CAPWAP reassembly function of the AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] np capwap-reassembly disable
```

11.2.149 np fast-forwarding disable (AP system profile view)

Function

The **np fast-forwarding disable** command disables the NP fast forwarding function of APs.

The **undo np fast-forwarding disable** command enables the NP fast forwarding function of APs.

By default, the NP fast forwarding function of APs is enabled.

NOTE

NP fast forwarding is supported only by the following APs:

- AirEngine 9700D-M, AirEngine 8760-X1-PRO, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD
- AirEngine 9700D-S (including matching ORUs)
- AirEngine 5762 series

Format

np fast-forwarding disable

undo np fast-forwarding disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

With the NP fast forwarding function, the NP replaces the CPU to forward some packets. This speeds up the packet processing and improves the forwarding performance.

Example

Disable the NP fast forwarding function of APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] np fast-forwarding disable
```

11.2.150 password alert before-expire (AP password policy view)

Function

The **password alert before-expire** command sets 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 *days*

undo password alert before-expire

Parameters

Parameter	Description	Value
days	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

AP password policy view

Default Level

3: Management level

Usage Guidelines

When a user logs in to the device, the device checks whether the validity period of the user's password is within the prompt days set by using this command. If so, the device prompts the user how long the password will expire and asks the user whether to change the password.

- If the user changes the password, the device records the new password and 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 does not expire.

Example

Set the number of password expiration prompt days to 90.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy] password alert before-expire 90
```

11.2.151 password alert original (AP password policy view)

Function

The **password alert original** command enables the device to prompt users to change initial passwords upon the login to an AP.

The **undo password alert original** command disables the device from prompting users to change initial passwords upon the login to an AP.

By default, the initial password change prompt function is enabled.

Format

password alert original

undo password alert original

Parameters

None

Views

AP password policy view

Default Level

3: Management level

Usage Guidelines

To improve device security, you can use this command to enable the device to prompt users to change initial passwords upon the login to the AP. Upon login to an AP, if the initial password is used, the system prompts users to change the password.

Executing the **undo password alert original** command will disable the initial password change prompt function upon the login to an AP, which will bring security risks.

Example

Enable the initial password change prompt function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy] password alert original
```

11.2.152 password expire (AP password policy view)

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 *days*

undo password expire

Parameters

Parameter	Description	Value
days	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

AP 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** to change the password, the user needs to enter the old password, new password, and confirm password. The password can be successfully changed only when the old password is correct and the new password and confirm password are the same and meet requirements (password length and complexity). After the password is changed, the user can log in to the device successfully.
- If the user selects **N** or fails to change the password, the 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 one minute; therefore, there may be a time difference within one minute.

Example

Set the password validity period to 120 days.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy] password expire 120
```


11.2.153 password history record number (AP password policy view)

Function

The **password history record number** command sets the maximum number of historical passwords recorded for each AP login user.

The **undo password history record number** command restores the default maximum number of historical passwords recorded for each user.

By default, a maximum of five historical passwords are recorded for each user.

Format

password history record number *number*

undo password history record number

Parameters

Parameter	Description	Value
number	Specifies the maximum number of historical passwords recorded for each user. If the value is set to 0, the device will not check whether a changed password is the same as any historical password.	The value is an integer that ranges from 0 to 12. The default value is 5.

Views

AP 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.

Example

Set the maximum number of historical passwords recorded for each AP login user to 10.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy] password history record number 10
```

11.2.154 pki realm (AP PKI realm profile view)

Function

The **pki realm** command configures a name for an AP PKI realm and binds the CA certificate, local certificate, CRL file, and private key file to the realm.

The **undo pki realm** command deletes the configuration of a PKI realm in an AP PKI realm profile.

By default, no name is configured for an AP PKI realm, and the CA certificate, local certificate, CRL file, and private key file are not bound to the realm.

Format

pki realm *realm-name* { { **ca format** { **der** *file-name* | **pem** *file-name* | **pkcs12** *file-name* **password** *password* } } | { **local format** { **der** *file-name* | **pem** *file-name* | **pkcs12** *file-name* **password** *password* } [**private-key format** { **der** *file-name* | **pem** *file-name* **password** *password* | **pkcs12** *file-name* **password** *password* }] } } *

undo pki realm *realm-name*

pki realm *realm-name* **crl-filename** *file-name*

undo pki realm *realm-name* **crl-filename**

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The value is a string of 1 to 50 case-sensitive characters without spaces.
ca	Specifies a CA certificate.	-
local	Specifies a local certificate.	-
private-key	Specifies the private key file of a local certificate.	-
format	Specifies the file format.	-

Parameter	Description	Value
der	Sets the file format to DER.	-
pkcs12	Sets the file format to PKCS12.	-
pem	Sets the file format to PEM.	-
file-name	Specifies the name of the CA certificate, local certificate, or private key file to be imported.	The value is a string of 1 to 50 case-sensitive characters without spaces.
password *password*	Specifies the decryption password of a private key file.	The password can be entered in plaintext or ciphertext: • A plaintext password is a string of 6 to 32 characters. • A ciphertext password is a string of 48 or 68 characters, and must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters.
crl-filename *file-name*	Specifies the name of a CRL file to be imported.	The value is a string of 1 to 50 case-sensitive characters without spaces.

Views

AP PKI realm profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the AP PKI realm profile view, configure a name for an AP PKI realm and bind the CA certificate, local certificate, CRL file, and private key file to the realm.

Prerequisites

1. An AP PKI realm profile has been created using the **ap-pki-profile (WLAN view)** command.

Follow-up Procedure

1. Run the **ap-pki-profile (AP group view and AP view)** command to bind the AP PKI realm profile to an AP or AP group.
2. Run the **load-file (WLAN view)** command to manually load a certificate file in the AP PKI realm to an AP.

Precautions

A maximum of five PKI realms can be configured in an AP PKI realm profile, and private keys can be configured in a maximum of three PKI realms. To check information about an AP PKI realm profile, run the **display ap-pki-profile** command.

To ensure network security, it is recommended that the public key length and private key length of a certificate file be greater than or equal to 3072 bits.

To update a certificate file, run the **load-file (WLAN view)** command to manually load the certificate file in the AP PKI realm to the AP. The latest configuration overrides the previous one.

Example

In the AP PKI realm profile **default**, set the PKI realm name to **r1**, and set the certificate files in the realm as follows: CA certificate file **1.txt** in **DER** format, local certificate file **2.txt** in **PEM** format, and private key file **3.txt** in **PEM** format (private key decryption password: **YsHsjx_202206**).

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-pki-profile name default
[HUAWEI-wlan-ap-pki-prof-default] pki realm r1 ca format der 1.txt local format pem 2.txt private-key format pem 3.txt password YsHsjx_202206
```

11.2.155 poe af-inrush enable (AP system profile view)

Function

The **poe af-inrush enable** command configures an AP to provide PoE power in compliance with IEEE 802.3af.

The **undo poe af-inrush enable** command restores the default PoE power supply standard of an AP.

By default, an AP provides PoE power in compliance with IEEE 802.3at.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe af-inrush enable

undo poe af-inrush enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AP that conforms to IEEE 802.3at cannot power non-IEEE standard PDs that do not support inrush current. To power these PDs, configure the AP to provide power with low current in conformance to IEEE 802.3af. When all PDs connected to the AP are IEEE standard-compliant PDs, run the **undo poe af-inrush enable** command to cancel the configuration.

Precautions

- The **poe af-inrush enable** command does not take effect on an interface if the **poe force-power (AP wired port link profile view)** command has been executed on the interface.
- After this command is configured, the AP cannot provide power for IEEE 802.3at-compliant PDs.

Configuration Impact

After running the **poe af-inrush enable** command, remove the non-IEEE 802.3at PDs and then install them so that the PDs can be powered on.

Example

Set the PoE power supply standard to IEEE 802.3af for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe af-inrush enable
```

11.2.156 poe disable (AP wired port link profile view)

Function

The **poe disable** command disables the PoE function on an AP's wired interface.

The **undo poe disable** command enables the PoE function on an AP's wired interface.

By default, the PoE function is enabled on an AP's interface.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe disable

undo poe disable

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using an AP to provide power for PDs connected to its interfaces, ensure that the PoE function is enabled on the interfaces. To enable the PoE function on an interface, run the **undo poe disable** command.

The power-on and power-off of interfaces are determined by the PoE power and interface power priority. When the PoE power is sufficient, the device does not power off one interface. To stop providing power for one PD, run the **poe disable** command.

Precautions

The AP only supports PoE power supply on downlink interfaces and does not support PoE power supply on uplink interfaces.

Example

Disable the PoE function on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] poe disable
```

11.2.157 poe force-power (AP wired port link profile view)

Function

The **poe force-power** command enables forcible PoE power supply on an interface.

The **undo poe force-power** command disables forcible PoE power supply on an interface.

By default, forcible PoE power supply is disabled on an interface.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe force-power

undo poe force-power

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this function is configured, an interface forcibly powers on the connected PD even if the PSE cannot identify the PD. Before powering on the interface, ensure that the system power is sufficient.

Precautions

If a PoE interface connects to a non-PoE device, use this command with caution.

Example

Enable forcible PoE power supply on an AP's interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] poe force-power
```

11.2.158 poe high-inrush enable (AP system profile view)

Function

The **poe high-inrush enable** command configures an interface to allow high inrush current during power-on.

The **undo poe high-inrush enable** command disables an interface from allowing high inrush current during power-on.

By default, interfaces do not allow high inrush current during power-on.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe high-inrush enable

undo poe high-inrush enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

High inrush current is generated when a non-standard PD is powered on. In this case, the PSE cuts off the power of the PD to protect itself. If the PSE is required to provide power for the PD, the PSE must allow high inrush current.

Precautions

NOTICE

The high inrush current may damage components of a PD.

Example

Enable the AP to allow high inrush current during power-on.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe high-inrush enable
```

11.2.159 poe legacy enable (AP wired port link profile view)

Function

The **poe legacy enable** command enables an AP to check compatibility of the connected PDs.

The **undo poe legacy enable** command disables an AP from checking compatibility of the connected PDs.

By default, an AP does not check compatibility of the connected PDs.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe legacy enable

undo poe legacy enable

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When compatibility check is enabled, an AP (PSE) can detect and provide power for the PDs incompliant with IEEE 802.3af or 802.3at. If compatibility check is disabled, the AP does not identify or provide power for these PDs.

Example

Enable an AP to check compatibility of the connected PDs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] poe legacy enable
```

11.2.160 poe max-power (AP system profile view)

Function

The **poe max-power** command sets the maximum output power of an AP.

The **undo poe max-power** command restores the maximum output power of an AP to the default value.

By default, the maximum output power of the AP is the total power that the PoE power supply provides for PDs.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe max-power *max-power*

undo poe max-power

Parameters

Parameter	Description	Value
max-power	Specifies the maximum output power of an AP.	The value ranges from 15400 mW to 750000 mW.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the system automatically obtains the maximum PoE power supported by the AP. You can run the **poe max-power** command to set the maximum output power to ensure stable PoE power supply when the total power of the AP is insufficient.

Precautions

If the maximum output power that you set is smaller than the total power required by PDs, PDs with lower priority are powered off.

The configured maximum output power must be smaller than the total power that the PoE power supply provides for PDs.

Example

Set the maximum output power of an AP to 20000 mW.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe max-power 20000
```

11.2.161 poe power-reserved (AP system profile view)

Function

The **poe power-reserved** command configures the percentage of the reserved PoE power against the total PoE power on an AP.

The **undo poe power-reserved** command restores the default percentage of the reserved PoE power against the total PoE power on an AP.

By default, the percentage of the reserved PoE power against the total PoE power on an AP is 0%.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe power-reserved *power-reserved*

undo poe power-reserved

Parameters

Parameter	Description	Value
power-reserved	Specifies the percentage of the reserved PoE power against the total PoE power.	The value is an integer that ranges from 0 to 100, in percentage.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AP can dynamically allocate power to each interface according to the power consumption of each interface. The power consumption of a PD keeps changing when the PD is running. The system periodically calculates the total power consumption of all the PDs. If the total power consumption exceeds the upper threshold of the AP, the system cuts off the power of the PDs on the interfaces of low priority to ensure that other PDs can run normally.

Sometimes, however, the power consumption increases sharply and the available power of the system cannot support the burst increase of power. At this time, the system has not calculated and found that the total power consumption exceeded the upper threshold; therefore, the system does not cut off power low-priority interfaces in time. As a result, the PoE power supply is shut down for overload protection, and all PDs are powered off.

This problem can be solved by running the **poe power-reserved** command to set proper reserved power. When there is a burst increase in power consumption, the

reserved power can support the system running. Then the system has time to power off interfaces of low priority to ensure stable running of other PDs.

Precautions

You can set the maximum output power of an AP using the **poe max-power (AP system profile view)** command. The available PoE power is the configured maximum output power. If no maximum output power is configured, the available PoE power is the total power provided by the PoE power supply.

Example

Set the percentage of reserved PoE power to the total PoE power to 10%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe power-reserved 10
```

11.2.162 poe power-threshold (AP system profile view)

Function

The **poe power-threshold** command sets the alarm threshold of the PoE power consumption percentage.

The **undo poe power-threshold** command restores the default alarm threshold of the PoE power consumption percentage.

By default, the alarm threshold is 100%.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe power-threshold *threshold-value*

undo poe power-threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold of the PoE power consumption percentage. When the power consumption reaches this value, a PoE power alarm is generated.	The value is an integer that ranges from 0 to 100, in percentage.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **poe power-threshold** command sets the alarm threshold of the PoE power consumption percentage. If the total PoE power is 380 W and the alarm threshold is 90%, an alarm is generated when the power consumption is greater than 342 W. When the power consumption falls below 342 W, the alarm is cleared.

Example

Set the alarm threshold of the PoE power consumption percentage to 80%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe power-threshold 80
```

11.2.163 poe priority (AP wired port link profile view)

Function

The **poe priority** command sets the power priority of a PoE interface.

The **undo poe priority** command restores the default power priority of a PoE interface.

By default, the power supply priority of an interface is **low**.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe priority { **critical** | **high** | **low** }

undo poe priority

Parameters

Parameter	Description	Value
critical	Indicates the highest priority.	-
high	Indicates the second highest priority.	-

Parameter	Description	Value
low	Indicates the lowest priority.	-

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the output power of a device is insufficient, the device provides power for the interfaces of the higher power supply priorities first and cuts off power of the interfaces of the lower power supply priorities. If all the interfaces are of the same priority, the power supply priority of the interface with a smaller interface number is higher.

Example

Set the power priority of an AP's interface to **Critical**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] poe priority critical
```

11.2.164 port-link-profile (WLAN view)

Function

The **port-link-profile** command creates an AP wired port link profile and displays the AP wired port link profile view, or displays the view of an existing AP wired port link profile.

The **undo port-link-profile** command deletes an AP wired port link profile.

By default, the system provides the AP wired port link profile **default**.

Format

port-link-profile name *profile-name*

undo port-link-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an AP wired port link profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all AP wired port link profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP wired port link profile offers link-layer management and configuration on AP's wired interfaces.

Follow-up Procedure

After you create an AP wired port link profile, run the **port-link-profile (AP wired port profile view)** command to bind it to an AP wired port profile and then run the **wired-port-profile (AP group view and view)** command to bind the AP wired port profile to an AP or AP group. In this way, the AP wired port link profile can take effect.

Precautions

- The AP wired port link profile **default** cannot be deleted.
- The AP wired port link profile referenced by an AP or AP group cannot be deleted. To delete the AP wired port link profile, unbind it from the AP or AP group first.

Example

Create the AP wired port link profile **port-link1** and display the AP wired port link profile view.

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



```
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1]
```

11.2.165 port-link-profile (AP wired port profile view)

Function

The **port-link-profile** command binds an AP wired port link profile to an AP wired port profile.

The **undo port-link-profile** command unbinds an AP wired port link profile from an AP wired port profile.

By default, the AP wired port link profile **default** is bound to an AP wired port profile.

Format

port-link-profile *profile-name*

undo port-link-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port link profile.	The AP wired port link profile must exist.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an AP wired port link profile using the **port-link-profile (WLAN view)** command, bind it to an AP wired port profile so that the AP wired port link profile can take effect.

Precautions

After an AP wired port link profile is bound to an AP wired port profile, parameter settings in the AP wired port link profile apply to specified interfaces of all APs using the AP wired port profile.

Example

Create the AP wired port link profile **port-link1** and bind it to the AP wired port profile **wired-port1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] quit
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] port-link-profile port-link1
```

11.2.166 port-security enable (AP wired port profile view)

Function

The **port-security enable** command enables the port security function on an interface.

The **undo port-security enable** command disables the port security function on an interface.

By default, port security is disabled on an interface.

Format

port-security enable

undo port-security enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. By default, secure dynamic MAC addresses will not be aged out. After the device restarts, secure dynamic MAC address entries are lost and need to be relearned.

- Prevent unauthorized users from using their computers to connect to an enterprise network.
- Prevent employees of a company from moving their computers without permission.

Precautions

The protection action, maximum number of learned secure MAC address entries, and sticky MAC function can be configured only after port security is enabled.

When the AP's wired interface works in root or middle mode, port security cannot be configured. Port security can be configured on an AP's wired interface only when the interface works in endpoint mode.

Example

Enable port security.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode con
figuration will cause the AP to go out of management. This fault can be recovere
d only by modifying the configuration on the AP. Continue? [Y/N]:y
Warning: This action will take effect after resetting AP.
[HUAWEI-wlan-wired-port-wire1] port-security enable
```

11.2.167 port-security mac-address sticky (AP wired port profile view)

Function

The **port-security mac-address sticky** enables the sticky MAC function on an interface.

The **undo port-security mac-address sticky** disables the sticky MAC function on an interface.

By default, the sticky MAC function is disabled on an interface.

Format

port-security mac-address sticky

undo port-security mac-address sticky

Parameters

None.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the port security function is enabled on an interface using the **port-security enable** command, the MAC addresses learned by the interface are converted into dynamic secure MAC addresses.

After the sticky MAC function is enabled on the interface, the dynamic secure MAC addresses learned by the interface are converted into sticky MAC addresses.

Before the number of sticky MAC addresses reaches the limit on the interface, the MAC addresses learned subsequently are still converted into sticky MAC addresses. When the number of sticky MAC addresses reaches the limit, non-sticky MAC addresses are discarded. In addition, the system determines whether to send a trap message based on the configuration of the interface protection mode.

Prerequisites

The port security function has been enabled using the **port-security enable** command on the interface.

Example

Enable the sticky MAC function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode con
figuration will cause the AP to go out of management. This fault can be recovere
d only by modifying the configuration on the AP. Continue? [Y/N]:y
Warning: This action will take effect after resetting AP.
[HUAWEI-wlan-wired-port-wire1] port-security enable
[HUAWEI-wlan-wired-port-wire1] port-security mac-address sticky
```

11.2.168 port-security max-mac-num (AP wired port profile view)

Function

The **port-security max-mac-num** command sets the maximum number of secure MAC addresses that can be learned by an interface.

By default, an interface can learn only one secure MAC address.

Format

port-security max-mac-num *max-number*

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of secure MAC addresses that can be learned by an interface.	The value is an integer that ranges from 1 to 64.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security on an interface, you can run the **port-security max-mac-num** command to limit the number of secure MAC addresses that can be learned by the interface bound to the AP wired port profile. After the number of secure MAC addresses exceeds the limit, the switch considers that packets with nonexistent source MAC addresses as attack packets regardless of whether the packets have destination MAC addresses. The device then takes the action specified using the **port-security protect-action** command to protect the interface. This prevents STAs with untrusted MAC addresses from communicating with the switch through this interface, improving security of the device and network.

If you run the **undo port-security enable** command to disable port security on an interface, the maximum number of secure MAC addresses that can be learned on the interface will be restored to the default value after port security is enabled again.

Prerequisites

The port security function has been enabled using the **port-security enable** command on the interface.

Precautions

If the sticky MAC function is disabled, *max-number* limits the number of secure dynamic MAC addresses learned by the interface.

If the sticky MAC function is enabled, *max-number* limits the number of sticky MAC addresses learned by the interface.

If you run the **port-security max-mac-num** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the maximum number of secure MAC addresses that can be learned by the interface bound to the AP wired port profile to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode con
figuration will cause the AP to go out of management. This fault can be recovere
d only by modifying the configuration on the AP. Continue? [Y/N]:y
Warning: This action will take effect after resetting AP.
[HUAWEI-wlan-wired-port-wire1] port-security enable
[HUAWEI-wlan-wired-port-wire1] port-security max-mac-num 5
```

11.2.169 port-security protect-action (AP wired port profile view)

Function

The **port-security protect-action** command configures a protection action for the system to perform when the number of learned MAC addresses exceeds the limit.

The **undo port-security protect-action** command restores the default protection action.

The default action is **restrict**.

Format

port-security protect-action { **protect** | **restrict** }

undo port-security protect-action

Parameters

Parameter	Description	Value
protect	Discards packets with new source MAC addresses when the number of learned MAC addresses exceeds the limit.	-
restrict	Discards packets with new source MAC addresses and sends a trap message when the number of learned MAC addresses exceeds the limit.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security, you can run the **port-security protect-action** command to configure the action performed on the interface when the number of learned MAC addresses reaches the limit.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

If you run the **port-security protect-action** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the protection action on an AP's wired interface to **protect**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode con
figuration will cause the AP to go out of management. This fault can be recovere
d only by modifying the configuration on the AP. Continue? [Y/N]:y
Warning: This action will take effect after resetting AP.
[HUAWEI-wlan-wired-port-wire1] port-security enable
[HUAWEI-wlan-wired-port-wire1] port-security protect-action protect
```

11.2.170 power force work-mode

Function

The **power force work-mode** command sets the power supply mode for APs.

The **undo power force work-mode** command restores the default power supply mode of APs.

By default, no power supply mode is configured for APs.

Format

power force work-mode { **af** | **at** | **bt60** | **bt90** }

undo power force work-mode

Parameters

Parameter	Description	Value
af	Sets the power supply mode to 802.3af.	-
at	Sets the power supply mode to 802.3at.	-
bt60	Sets the power supply mode to 802.3bt class 6.	-
bt90	Sets the power supply mode to 802.3bt class 8. **NOTE** The parameters **bt60** and **bt90** are valid only for APs that support 802.3bt PoE power supply.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the power supply mode of an AP cannot be correctly identified through LLDP or hardware, you can run the **power force work-mode** command to manually adjust the PoE power supply mode of the AP so that the AP can work in the specified power supply mode.

Configuration Impact

The power supply mode configured using the **power force work-mode** command takes effect for the logic of reducing power consumption on the APs. If this command is not configured, the power supply mode identified by LLDP or hardware is used.

If an AP's input power is low (for example, the power supply mode is 802.3at) but the power supply mode is manually set to 802.3bt class 8 (**bt90**), the AP will work in 802.3bt class 8 mode, which may cause a power failure.

If an AP's input power is high (for example, the power supply mode is 802.3bt class 8) but the power supply mode is manually set to 802.3at, the AP cannot work properly due to insufficient power.

Running this command may interrupt services.

Example

Set the power supply mode for APs to **802.3at**.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] power force work-mode at
Warning: If the PSE does not reach the target power supply level, executing this command may cause the
AP to repeatedly restart due to insufficient power. Continue? [Y/N]: y
```

11.2.171 provision-ap

Function

The **provision-ap** command displays the AP provisioning view.

Format

provision-ap

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

In the AP provisioning view, you can configure provisioning parameters of APs, including the management VLAN, static IP address, gateway, and AC list, which facilitates remote AP management on the AC.

Example

Display the AP provisioning view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap]
```

11.2.172 reset ap-type undefined record

Function

The **reset ap-type undefined record** command clears the types of the APs that fail to connect to an AC because the AC does not support these AP types.

Format

reset ap-type undefined record

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to clear the types of the APs that fail to connect to an AC because the AC does not support these AP types.

The cleared records cannot be restored.

Example

Clears the types of the APs that fail to connect to the AC because the AC does not support these AP types.

```
<HUAWEI> reset ap-type undefined record
```

11.2.173 reset mac-address

Function

The **reset mac-address** command deletes all dynamic, dynamic secure, and sticky MAC address entries from an AP's wired interface.

Format

reset mac-address { **ap-id** *ap-id* | **ap-name** *ap-name* } *interface-type interface-number*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Deletes all dynamic, dynamic secure, and sticky MAC address entries from the wired interface of the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
ap-name *ap-name*	Deletes all dynamic, dynamic secure, and sticky MAC address entries from the wired interface of the AP with a specified name.	The AP name must exist.
interface-type interface-number	Deletes all dynamic, dynamic secure, and sticky MAC address entries from a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the number of the outbound interface.	The following types of outbound interfaces are supported: • Eth-Trunk • Ethernet • Gigabitethernet • MultiGE • XGigabitethernet

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **reset mac-address** command to delete all dynamic MAC address entries from an AP's wired interface. If the port security and sticky MAC functions are enabled, dynamic secure MAC address and sticky MAC address entries are also deleted.

Example

Delete all dynamic, dynamic secure, and sticky MAC address entries from the wired interface of the AP with ID 0.

```
<HUAWEI> reset mac-address ap-id 0 ethernet 0
```

11.2.174 reset statistics

Function

The **reset statistics** command clears device statistics.

Format

reset statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } [**ssid** *ssid*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Clears statistics about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Clears statistics about the AP with a specified ID.	The AP ID must exist.
ssid *ssid*	Clears statistics about a specified SSID.	The SSID must exist. To specify an SSID starting with a space, include the SSID with double quotation marks (" "). For example, in the SSID **" hello"**, the double quotation marks at the start and end of the SSID occupy two characters. To specify an SSID starting with a double quotation mark ("), enter an escape character (\) before the double quotation mark. For example, in the SSID **\"hello**, the escape character (\) occupies one character.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

You can run the **reset statistics** command to clear device statistics.

Example

Clear AP statistics.


```
<HUAWEI> system view
[HUAWEI] wlan
[HUAWEI-wlan-view] reset statistics ap-name area1
```

11.2.175 reset wlan console ble statistics

Function

The **reset wlan console ble statistics** command clears statistics about Bluetooth-based console port login on an AP.

NOTE

The following models do not support the Bluetooth serial port function:

- AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
- AirEngine 5762-10 and AirEngine 5762-10SW
- AirEngine 9700D-M and AirEngine 9700D-M1

Format

reset wlan console ble statistics { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to clear statistics about Bluetooth-based console port login on an AP.

Example

Clear statistics about Bluetooth-based console port login on an AP named **huawei**.

```
<HUAWEI> reset wlan console ble statistics ap-name huawei
```


11.2.176 sample-time

Function

The **sample-time** command sets the sampling interval for an AP.

The **undo sample-time** command restores the default sampling interval of an AP.

The default sampling interval of an AP is 30s.

Format

sample-time *sample-time*

undo sample-time

Parameters

Parameter	Description	Value
sample-time	Specifies the sampling interval.	The value is an integer that ranges from 2 to 300, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP collects statistics on data including AP-based, radio-based, and STA-based data. Collected STA-based data statistics only include those that can be displayed using the **display** command on the AC.

Example

Set the sampling interval to 50s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] sample-time 50
```


11.2.177 sftp server disable

Function

The **sftp server disable** command disables the SFTP server function on an AP.

The **undo sftp server disable** command enables the SFTP server function on an AP.

By default, the SFTP server function is enabled on an AP.

Format

sftp server disable

undo sftp server disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You do not need to log in to an SFTP-enabled AP from a user terminal for file management. Instead, you can log in to the SFTP-enabled AP through SFTP to manage files of the AP.

Example

Disable the SFTP server function on an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] sftp server disable
```

11.2.178 shutdown (AP wired port link profile view)

Function

The **shutdown** command shuts down an AP's wired interface.

The **undo shutdown** command enables an AP's wired interface.

By default, an AP's wired interface is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If malicious users launch attacks to the network through an AP's wired interface, the administrator can deliver the **shutdown** command on the AC to shut down the interface.

Precautions

Data frames may be lost if you shut down an interface during data transmission. Exercise caution when you use the **shutdown** command.

The **shutdown** command still takes effect after an AP is restarted.

The **shutdown** command takes effect only on AP's wired interfaces working in **endpoint** or **middle** mode but not on those working in **root** mode.

Example

Shut down the AP's wired interface GE0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] shutdown
Warning: This command does not take effect for root interfaces.
[HUAWEI-wlan-port-link-prof-port-link1] quit
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] port-link-profile port-link1
[HUAWEI-wlan-wired-port-wired-port1] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired-port1 gigabitethernet 0
```

11.2.179 ssh client first-time enable (AP system profile view)

Function

The **ssh client first-time enable** command enables the first authentication on the SSH client.

The **undo ssh client first-time enable** command disables the first authentication on the SSH client.

By default, the first authentication is disabled on the SSH client.

Format

ssh client first-time enable

undo ssh client first-time enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the SSH client accesses the SSH server for the first time and the public key of the SSH server is not configured on the SSH client, you can enable the first authentication for the SSH client to access the SSH server and save the public key of the SSH server on the SSH client. When the SSH client accesses the SSH server next time, the saved public key of the SSH server is used to authenticate the SSH server.

Example

Enable the first authentication on the SSH client.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] ssh client first-time enable
```

11.2.180 speed (AP wired port link profile view)

Function

The **speed** command sets the rate for an AP's wired interface in non-auto negotiation mode.

The **undo speed** command restores the default rate of an AP's wired interface.

By default, an AP's wired interface works in auto-negotiation mode, and its rate is negotiated with the peer interface.

Format

speed { **100** | **1000** | **2500** | **5000** | **10000** }

undo speed

Parameters

Parameter	Description	Value
100	Sets the interface rate to 100 Mbit/s.	-
1000	Sets the interface rate to 1000 Mbit/s. **NOTE** FE electrical interfaces do not support this parameter.	-
2500	Sets the interface rate to 2500 Mbit/s. **NOTE** Only multi-GE interfaces support this parameter.	-
5000	Sets the interface rate to 5000 Mbit/s. **NOTE** Only multi-GE interfaces support this parameter.	-
10000	Sets the interface rate to 10000 Mbit/s. **NOTE** Only XGE interfaces support this parameter.	-

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the peer interface is configured with the forcible rate, you can run this command to set the rate of the corresponding interface on the local AP to prevent communication failures.

Precautions

- Exercise caution when running this command. The default value for this command is recommended unless otherwise required. If this configuration is mandatory, do not run this command in the **default** profile to prevent the configuration from being delivered to all interfaces.
- This command is available only on the FE, GE, multi-GE, and XGE interfaces on an AP but does not take effect on other types of interfaces.
- After the **speed** command is run, the AP changes the working mode of the interface to non-auto-negotiation and changes the interface rate based on the configuration. During this process, the interface may go Down or Up. Therefore, the configuration delivery takes a long time.
- After running the **speed** command to change the negotiation mode and rate of an AP's wired interface, ensure that the remote interface works in full-duplex mode and has the same rate as the local interface; otherwise, communication is affected.

Example

Set the rate of an AP's wired interface to 100 Mbit/s in non-auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] speed 100
Warning: This operation may interrupt user services. If the AP works at the power derating mode, the configuration may fail to take effect because the rate limit is exceeded, Continue? [Y/N]:y
```

11.2.181 stelnet server disable

Function

The **stelnet server disable** command disables the STelnet server function on an AP.

The **undo stelnet server disable** command enables the STelnet server function on an AP.

By default, the STelnet server function is enabled on an AP.

Format

stelnet server disable

undo stelnet server disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You do not need to log in to an STelnet-enabled AP from a user terminal to maintain it locally. Instead, you can log in to the STelnet-enabled AP through STelnet to remotely configure and maintain it.

Example

Disable the STelnet server function on an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] stelnet server disable
```

11.2.182 stp auto-shutdown enable (AP wired port profile view)

Function

The **stp auto-shutdown enable** command enables the STP-triggered port shutdown function on an AP's wired interface.

The **undo stp auto-shutdown enable** command disables the STP-triggered port shutdown function on an AP's wired interface.

By default, the STP-triggered port shutdown function is disabled on an AP's wired interface.

Format

stp auto-shutdown enable

undo stp auto-shutdown enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STP-triggered port shutdown function is enabled, the AP automatically shuts down the interface when STP detects a loop. The AP will periodically recover the interface and re-executes STP detection. If the loop still exists on the interface,

the AP shuts down the interface again. If the loop is removed, the AP reports a clear alarm to the network management system (NMS).

Prerequisites

STP has been enabled on the AP's wired interface using the **stp enable (AP wired port profile view)** command.

Precautions

The AP wired interfaces added to an Eth-trunk do not support this function.

This function is supported only when a loop exists on the network connected to the AP's wired port, that is, a port receives STP packets sent by itself.

Example

Disable the STP-triggered port shutdown function on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] stp auto-shutdown enable
Warning: The AP may become out of management after the STP-triggered port shutdown function is
enabled (if the port is an uplink por
t). Continue?[Y/N]:y
```

11.2.183 stp auto-shutdown recovery-time (AP wired port profile view)

Function

The **stp auto-shutdown recovery-time** command sets an auto-recovery interval for an AP's wired interface on which the STP-triggered port shutdown function is enabled.

The **undo stp auto-shutdown recovery-time** command restores the default auto-recovery interval for an AP's wired interface on which the STP-triggered port shutdown function is enabled.

By default, the auto-recovery interval is 600s.

Format

stp auto-shutdown recovery-time *recovery-time*

undo stp auto-shutdown recovery-time

Parameters

Parameter	Description	Value
recovery-time	Specifies the auto-recovery interval for an AP's wired interface on which the STP-triggered port shutdown function is enabled.	The value is an integer that ranges from 600 to 3600, in seconds.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STP-triggered port shutdown function is enabled, the AP automatically shuts down the interface when STP detects a loop. The AP will periodically recover the interface and re-executes STP detection. If the loop still exists on the interface, the AP shuts down the interface again. If the loop is removed, the AP reports a clear alarm to the network management system (NMS).

Prerequisites

The STP-triggered port shutdown function has been enabled on the AP's wired interface using the **stp auto-shutdown enable (AP wired port profile view)** command.

Precautions

The AP wired interfaces added to an Eth-trunk do not support this function.

Example

Set the auto-recovery interval to 800s for an AP's wired interface on which the STP-triggered port shutdown function is enabled.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] stp auto-shutdown recovery-time 800
```

11.2.184 stp enable (AP wired port profile view)

Function

The **stp enable** command enables STP on an AP's wired interface.

The **stp disable** command disables STP on an AP's wired interface.

The **stp auto** command configures STP in auto-sensing mode on an AP's wired interface.

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

By default, STP works in auto-sensing mode on an AP's wired interface.

Format

stp enable

stp disable

stp auto

undo stp

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **stp enable** command to prevent or eliminate loops on a complex Layer 2 network. STP on the AP's wired interfaces takes effect only when the AP forms a single loop with wired devices. Wireless links (such as WDS or Mesh links) only transparently forward STP BPDUs. An STP-enabled AP does not forward STP BPDUs to the wireless side. STP takes effect only on the AP's wired side.

When the STP function of an AP's wired interface is in auto-sensing mode, downlink interfaces of wall plate APs and RUs are enabled with the STP function and serve as edge interfaces, but STP is disabled on wired interfaces of other APs.

Precautions

The AP wired interfaces added to an Eth-Trunk do not support STP.

Example

Enable STP on the AP's wired interface GE0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] stp enable
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.185 telnet enable

Function

The **telnet enable** command enables Telnet on an AP.

The **undo telnet enable** command disables Telnet on an AP.

By default, Telnet is disabled on an AP.

Format

telnet enable

undo telnet enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You do not need to log in to a Telnet-enabled AP from a user terminal to maintain it locally. Instead, you can log in to the Telnet-enabled AP through Telnet to remotely configure and maintain it.

To improve login security, you are advised to run the **undo stelnet server disable** command to enable the STelnet server function and log in to the AP through STelnet.

Example

Enable Telnet on an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] telnet enable
```

11.2.186 temporary-management disable (AP system profile view)

Function

The **temporary-management disable** command disables the offline management VAP and antenna alignment VAP functions of APs.

The **undo temporary-management disable** command enables the offline management VAP and antenna alignment VAP functions of APs.

By default, the offline management VAP and antenna alignment VAP functions of APs enabled.

NOTE

The antenna alignment VAP function is not supported by AirEngine series APs.

Format

temporary-management disable

undo temporary-management disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- APs are often installed in hidden places or at high positions. When an AP becomes faulty, it is inconvenient to connect to the AP through a console port or network cable to troubleshoot faults.

  After the offline management VAP function is configured, if an AP goes offline unexpectedly, maintenance personnel only need to set the IP address of a STA to 169.254.2.*x*/24 (except 169.254.2.1, 169.254.2.100 is recommended). After the STA associates with the offline management VAP, maintenance personnel can connect the STA to the AP in Telnet or STelnet mode to locate and rectify faults, saving the need to connect to the AP through the console port or a network cable.
- During WDS or Mesh network deployment, you can configure antenna alignment VAPs for WDS or Mesh nodes to facilitate antenna alignment between neighboring APs. During onsite commissioning, you can use a mobile terminal to connect to the antenna alignment VAP and enable CloudCampus APP to obtain information such as the signal strength of the peer AP's radio. Based on the obtained information, you can easily complete antenna alignment. The SSID of the generated antenna alignment VAP is hidden and will be automatically deleted 24 hours after being created.

After the offline management VAP and antenna alignment VAP functions are configured, the VAP generated when an AP goes offline is an offline management VAP. When the AP works properly, the VAP generated in the WDS or Mesh scenario is an antenna alignment VAP.

The offline management VAP and antenna alignment VAP functions can be configured in either of the following ways:

- Configure the default offline management VAP and antenna alignment VAP. After the offline management VAP and antenna alignment VAP functions are enabled using this command, an AP automatically creates a management VAP when the AP goes offline unexpectedly. The default SSID of this VAP is **hw_manage_xxxx**, where **xxxx** is the last 4 digits of the AP's MAC address. When an AP works properly in a WDS or Mesh scenario, it automatically

creates an antenna alignment VAP. The default SSID of this VAP is **hw_manage_xxxx**, where **xxxx** is the last 4 digits of the AP's MAC address.

- Create an offline management VAP and antenna alignment VAP. Any STA can use the default SSID and password to log in to an AP, which poses security risks. To improve the security of the offline management VAP and antenna alignment VAP, you can bind a security profile of a high security level to a VAP profile, and set a new SSID and password. Additionally, you can run the **temporary-management enable** command in the VAP profile view and the **undo temporary-management disable** command in the AP system profile view to configure the VAPs generated by the VAP profile as the offline management VAP and antenna alignment VAP. The default offline management VAP and antenna alignment VAP will not be created.

Precautions

- The offline management VAP takes effect only when an AP goes offline unexpectedly.
- The offline management VAP function does not take effect on 4.9 GHz radios.
- Before using the offline management VAP function, ensure that the AP has enabled with Telnet or STelnet services.
- The antenna alignment VAP is automatically deleted 24 hours after it is created. To use the deleted antenna alignment VAP, run the **temporary-management disable** command and then the **undo temporary-management disable** command in the AP system profile view to create an antenna alignment VAP again.
- After the offline management VAP function is enabled:
  - If the link between the central AP and RUs is disconnected, the RUs will not generate an offline management VAP.
  - If the link between the central AP and AC is disconnected but RUs are still connected to the central AP, all online RUs connected to the central AP automatically generate an offline management VAP. If an AD9431DN-24X or AirEngine 9700D-M is used as the central AP, STAs log in to RUs through the offline management VAP. If a central AP other than the AD9431DN-24X or AirEngine 9700D-M is used, STAs log in to the central AP through the offline management VAP.
- The central AP does not have radios and therefore do not generate an offline management VAP.
- In offline management VAP scenarios, STA address learning does not take effect.

Example

Enable the offline management VAP and antenna alignment VAP function of APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] undo temporary-management disable
```


11.2.187 temporary-management enable (VAP profile view)

Function

The **temporary-management enable** command configures a VAP as the offline management VAP and antenna alignment VAP.

The **undo temporary-management enable** command restores a VAP to the default setting.

By default, a VAP is a service VAP.

NOTE

The antenna alignment VAP function is not supported by AirEngine series APs.

Format

temporary-management enable

undo temporary-management enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- After the offline management VAP function is enabled using the **undo temporary-management disable** command in the AP system profile view, an AP automatically generates an offline management VAP when it becomes faulty. The default SSID of the offline management VAP **hw_manage_xxxx**, where **xxxx** is the last 4 digits of the AP's MAC address. The maintenance personnel can associate the maintenance device with the default VAP and log in to the AP using Telnet or STelnet to troubleshoot the fault. However, using the default management VAP brings security risks. Any wireless user may use the default SSID and password to log in to the offline AP and perform unauthorized operations.
- After the antenna alignment VAP function is enabled using the **undo temporary-management disable** command in the AP system profile view, an AP automatically generates an antenna alignment VAP when it works properly. The default SSID of the antenna alignment VAP is **hw_manage_xxxx**. **xxxx** indicates the last 4 digits of the AP's MAC address. Using the default antenna alignment VAP also brings security risks.

The default username and password are available in *WLAN 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.

To improve the security of the offline management VAP and antenna alignment VAP, you can bind a security profile of a high security level to a VAP profile, set a new SSID and password, configure the VAP generated by the VAP profile as the offline management VAP and antenna alignment VAP, and bind the VAP profile to an AP group or AP to replace the default offline management VAP and antenna alignment VAP.

Follow-up Procedure

After a VAP is configured as the offline management VAP and antenna alignment VAP in a VAP profile, run the **undo temporary-management disable** command in the AP system profile view to configure the offline management VAP and antenna alignment VAP functions of APs so that the offline management VAP and antenna alignment VAP functions of APs in the VAP profile can take effect.

Precautions

- If the VAPs are configured as the offline management VAP and antenna alignment VAP in a VAP profile, the security profile referenced by the VAP profile supports only the WEP or WPA/WPA2/WPA-WPA2 PSK security policy.
- If the VAPs are configured as the offline management VAP and antenna alignment VAP in a VAP profile, VAPs generated by the VAP profile cannot be used as service VAPs for service transmission.
- The offline management VAP and antenna alignment VAP of APs cannot be dynamically modified. To modify the VAPs, delete them first, and then modify the VAP attributes in the VAP profile view.
- The offline management VAP function does not take effect on 4.9 GHz radios.
- In offline management VAP scenarios, STA address learning does not take effect.

Example

Configure the VAP generated by the VAP profile **vap1** as the offline management VAP and antenna alignment VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] temporary-management enable
```

11.2.188 temporary-management psk

Function

The **temporary-management psk** command configures the login password for the offline management VAP and antenna alignment VAP.

The **undo temporary-management psk** command restores the preset password of the offline management VAP and antenna alignment VAP.

By default, no login password is configured, and the global password is in effect.

Format

temporary-management psk *psk-value*

undo temporary-management psk

Parameters

Parameter	Description	Value
psk-value	Specifies the login password of the offline management VAP and antenna alignment VAP.	The value is a string of 48 to 108 characters in ciphertext or a string of 8 to 63 characters in plaintext. The password must contain at least two types of uppercase letters, lowercase letters, digits, and special characters.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure the login password of the offline management VAP and antenna alignment VAP. If this password has not been configured, the global password is used by default, which is configured using the **temporary-management psk** (WLAN view) command. The password configured in the AP system profile has a higher priority than that configured in the WLAN view.

Example

Set the login password of the offline management VAP and antenna alignment VAP to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name default
[HUAWEI-wlan-ap-system-prof-default] temporary-management psk YsHsjx_202206
```


11.2.189 traffic-filter (AP wired port profile view)

Function

The **traffic-filter** command configures ACL-based IPv4, IPv6, or Layer 2 packet filtering on an AP's wired interface.

The **undo traffic-filter** command cancels the ACL-based IPv4, IPv6, or Layer 2 packet filtering configuration on an AP's wired interface.

By default, ACL-based IPv4, IPv6, or Layer 2 packet filtering is not configured on an AP's wired interface.

Format

traffic-filter { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

traffic-filter { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based packet filtering in the inbound direction.	-
outbound	Configures ACL-based packet filtering in the outbound direction.	-
ipv4	Configures ACL-based IPv4 packet filtering.	-
l2	Configures ACL-based Layer 2 packet filtering.	-
ipv6	Configures ACL-based IPv6 packet filtering.	-
acl	Filters packets based on the ACL.	-

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031 for IPv4 ACLs and IPv6 ACLs and from 4000 to 4031 for Layer 2 ACLs. ● 3000 to 3031: advanced ACLs ● 4000 to 4031: Layer 2 ACLs
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The ACL name must exist. The value range is the same as that of the *acl-number* parameter.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a wireless network, administrators want to provide differentiated services for wireless users. The services may include, but are not limited to the following:

- Deny or permit access of specified wireless users to specified LAN devices.
- Deny access of specified wireless users to specified invalid IP addresses.

You can configure ACL-based packet filtering on an AP's wired interface for providing differentiated services.

The rules for an AP's wired interface to filter packets based on ACLs are as follows:

- If the action in an ACL rule is **deny**, the device discards packets matching the rule.
- If the action in an ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

When multiple commands are configured for ACL-based packet filtering in the same direction in the same AP wired port profile view, packets are matched against ACL rules in the sequence in which the commands are configured. If packets match a rule, the system stops the matching process and executes the specified policy. Otherwise, the system continues to match packets against the

next rule. If no rule is matched, packets are allowed to pass through. The following occurs depending on whether packets match ACL rules:

- If a policy contains only one ACL rule and the ACL rule is matched, the **permit** or **deny** action is performed.
- If a policy contains two ACL rules and the specified action is performed only when the two ACL rules are both matched.

  If the actions in the two ACL rules are both **permit**, the **permit** action is performed. Otherwise, the **deny** action is performed.

If an ACL contains multiple rules, packets are matched against the rules in the ascending order of rule IDs.

Prerequisites

A named ACL has been created using the **acl name** or **acl name** command.

Precautions

You can specify an empty ACL in this command, and configure this ACL later.

A maximum of eight ACL-based packet filtering policies can be configured in one direction. The policies take effect in the sequence in which they are configured. To improve match efficiency, you are advised to configure an ACL rule with a high match probability for packet filtering. When configuring each ACL rule, set a small ID for the rule with a high match probability, reducing the number of times ACL rules are matched and saving resources. To change the sequence in which packets are filtered based on ACLs, delete all related configurations and reconfigure ACL-based packet filtering.

Example

Configure the wired interface GE0 on APs in an AP group to filter incoming packets based on ACL 3000.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] traffic-filter inbound ipv4 acl 3000
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.190 traffic-remark (AP wired port profile view)

Function

The **traffic-remark** command configures ACL-based priority re-marking on an AP's wired interface.

The **undo traffic-remark** command cancels the ACL-based priority re-marking configuration on an AP's wired interface.

By default, ACL-based priority re-marking is not configured on an AP's wired interface.

Format

traffic-remark { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* } { **dot1p** *dot1p-value* | **dscp** *dscp-value* }

undo traffic-remark { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

traffic-remark { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* } { **dot1p** *dot1p-value* | **dscp** *dscp-value* }

undo traffic-remark { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based priority re-marking in the inbound direction.	-
outbound	Configures ACL-based priority re-marking in the outbound direction.	-
ipv4	Configures priority re-marking for IPv4 packets.	-
ipv6	Configures priority re-marking for IPv6 packets.	-
l2	Configures priority re-marking for Layer 2 packets.	-
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031 for IPv4 ACLs and IPv6 ACLs and from 4000 to 4031 for Layer 2 ACLs. • 3000 to 3031: advanced ACLs • 4000 to 4031: Layer 2 ACLs
name *acl-name*	Re-marks packet priorities based on a specified named ACL. *acl-name* indicates an ACL name.	The value is a string of 1 to 32 case-sensitive characters without spaces and must begin with a letter. The value range of *acl-number* corresponding to *acl-name* is 3000 to 3031 and 4000 to 4031.

Parameter	Description	Value
dot1p *dot1p-value*	Re-marks the 802.1p priority of packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
dscp *dscp-value*	Re-marks the DSCP priorities of packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The user wants to re-mark packet priorities based on ACLs to provide differentiated services. The **traffic-remark** command can be used to configure ACL-based priority re-marking.

Prerequisites

An ACL rule has been created before this command is run.

- **acl (system view)**
- **acl ipv6 (system view)**
- **acl name**
- **acl ipv6 name**

Precautions

The **traffic-remark** command can reference a numbered ACL rule that is not configured. You can configure the referenced ACL rule after running this command.

You can only configure a maximum of eight ACL-based packet re-marking rules in the same direction. The sequence in which ACL rules takes effect follows the rule configuration sequence. To change the current packet re-marking rules, delete all the related configurations and reconfigure the ACL-based packet re-marking.

When the **traffic-remark** command and the **traffic-filter (AP wired port profile view)** command are used simultaneously and the same ACL rule is associated:

- If the **deny** action is configured in the ACL rule, the **traffic-remark** command does not take effect.

- If the **permit** action is configured in the ACL rule, the command that is executed first takes effect.

Example

Configure the wired interface GE0 of **ap-group1** and configure ACL-based 802.1p priority re-marking for IPv4 packets in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] traffic-remark inbound ipv4 acl 3000 dot1p 7
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.191 traffic-optimize (AP wired port profile view)

Function

The **traffic-optimize** command sets the maximum volume of broadcast, multicast, or unknown unicast traffic on an AP's wired interface.

The **undo traffic-optimize** command restores the default maximum volume of broadcast, multicast, or unknown unicast traffic on an AP's wired interface.

By default, the volume of broadcast, multicast, or unknown unicast traffic is not suppressed on an AP's wired interface.

Format

traffic-optimize { **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** } **packets** *packets-rate*

undo traffic-optimize { **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** }

Parameters

Parameter	Description	Value
broadcast-suppression	Specifies the maximum broadcast traffic volume that can be received on an AP's wired interface.	-
multicast-suppression	Specifies the maximum multicast traffic volume that can be received on an AP's wired interface.	-

Parameter	Description	Value
unicast-suppression	Specifies the maximum unknown unicast traffic volume that can be received on an AP's wired interface.	-
packets *packets-rate*	Specifies the maximum number of packets that can pass every second.	The value is an integer that ranges from 0 to 14881000, in pps.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of broadcast, multicast, and unknown unicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected. When the traffic volume of broadcast, multicast, and unknown unicast packets reaches the maximum on an AP's wired interface, the system discards excess packets to control the traffic volume in a proper range and prevent flooding attacks.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

The uplink interfaces of RUs do not support this command.

This command takes effect only for incoming traffic on an AP's wired interface.

Example

Set the maximum broadcast traffic volume that can be received on an AP's wired interface to 21600 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] traffic-optimize broadcast-suppression packets 21600
```

11.2.192 traffic-optimize broadcast-suppression disable (AP system profile view)

Function

The **traffic-optimize broadcast-suppression disable** command disables rate limiting for broadcast and multicast packets on an AP.

The **undo traffic-optimize broadcast-suppression disable** command enables rate limiting for broadcast and multicast packets on an AP.

By default, rate limiting for broadcast and multicast packets is enabled on an AP.

Format

traffic-optimize broadcast-suppression { **all** | **arp** | **igmp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **other-broadcast** | **other-multicast** } **disable**

undo traffic-optimize broadcast-suppression { **all** | **arp** | **igmp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **other-broadcast** | **other-multicast** } **disable**

Parameters

Parameter	Description	Value
all	Enables or disables rate limiting for ARP, IGMP, ND, DHCP, DHCPv6, and mDNS multicast and broadcast packets.	-
arp	Enables or disables rate limiting for ARP multicast packets.	-
igmp	Enables or disables rate limiting for IGMP multicast packets.	-
nd	Enables or disables rate limiting for ND broadcast packets.	-
dhcp	Enables or disables rate limiting for DHCP broadcast packets.	-
dhcpv6	Enables or disables rate limiting for DHCPv6 broadcast packets.	-
mdns	Enables or disables rate limiting for mDNS multicast packets.	-

Parameter	Description	Value
other-broadcast	Enables or disables rate limiting for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Enables or disables rate limiting for multicast packets other than IGMP and mDNS packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When an AP receives an increasing number of packets, more network resources are occupied and services on the network are affected. To ensure normal running of network services, you can limit the rate of some protocol packets (such as DHCP and ARP packets) on an AP to a proper range.

You can run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command to configure a rate limit threshold for broadcast and multicast packets of an AP, which will override the default rate threshold.

Precautions

When multicast services are enabled, the multicast services may be affected if rate limiting for multicast packets is enabled on an AP. In this case, you are advised to run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command to adjust the rate limit threshold for multicast packets.

Rate limiting for broadcast and multicast packets takes effect only for incoming traffic on an AP's wired interface.

Example

Enable rate limiting for ARP broadcast packets in AP system profile **system1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] undo traffic-optimize broadcast-suppression arp disable
```

11.2.193 traffic-optimize broadcast-suppression rate-threshold (AP system profile view)

Function

The **traffic-optimize broadcast-suppression rate-threshold** command sets a rate limit threshold for broadcast and multicast packets on an AP.

The **undo traffic-optimize broadcast-suppression rate-threshold** command restores the default rate limit threshold of broadcast and multicast packets on an AP.

By default, the rate limit threshold for **other-broadcast** and **other-multicast** is 16 pps, and that for other parameters is 256 pps.

Format

traffic-optimize broadcast-suppression { **arp** | **igmp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **other-broadcast** | **other-multicast** } **rate-threshold** *threshold-value*

undo traffic-optimize broadcast-suppression { **arp** | **igmp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **other-broadcast** | **other-multicast** } **rate-threshold**

Parameters

Parameter	Description	Value
arp	Specifies ARP broadcast packets.	-
igmp	Specifies IGMP multicast packets.	-
nd	Specifies ND broadcast packets.	-
dhcp	Specifies DHCP broadcast packets.	-
dhcpv6	Specifies DHCPv6 broadcast packets.	-
mdns	Specifies mDNS multicast packets.	-
other-broadcast	Specifies broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Specifies multicast packets other than IGMP and mDNS packets. **NOTE** If **other-multicast** is specified, LLDPDUs are not rate-limited.	-

Parameter	Description	Value
rate-threshold *threshold-value*	Specifies a rate limit threshold.	For **arp**, **nd**, **dhcp**, and **dhcpv6**, the value is an integer that ranges from 64 to 1024, in pps. The default value is 256. For **igmp** and **mdns**, the value is an integer that ranges from 0 to 1024, in pps. The default value is 256. For **other-broadcast** and **other-multicast**, the value is an integer that ranges from 0 to 1024, in pps. The default value is 16.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before setting a rate limit threshold for broadcast and multicast packets, run the **undo traffic-optimize broadcast-suppression disable** command to enable rate limiting for broadcast and multicast packets.

After you run the **traffic-optimize broadcast-suppression rate-threshold** command to configure a rate limit threshold for broadcast and multicast packets on an AP, the configured threshold will override the default rate limit threshold. The actual rate of broadcast and multicast packets will not exceed the configured rate limit threshold. If a large rate limit threshold is set, the expected network protection effect is not achieved. If a small rate limit threshold is set, broadcast and multicast packets may be lost. In most cases, use the default rate limit threshold unless otherwise specified.

Precautions

Rate limiting for broadcast and multicast packets takes effect only for incoming traffic on an AP's wired interface.

The rate limit threshold for multicast and broadcast packets applies to the inbound direction on all AP wired interfaces. That is, the rate of multicast and broadcast packets is limited only when the total rate of multicast and broadcast packets in the inbound direction of all AP wired interfaces exceeds the rate limit.

Example

Set the rate limit threshold for ARP broadcast packets in AP system profile **system1** to 300 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] undo traffic-optimize broadcast-suppression all disable
[HUAWEI-wlan-ap-system-prof-system1] traffic-optimize broadcast-suppression arp rate-threshold 300
```

11.2.194 undo capwap dtls server-auth (AP view)

Function

The **undo capwap dtls server-auth** command restores the default state of the AC authentication function for APs.

By default, the AC authentication function for APs is disabled.

Format

undo capwap dtls server-auth

Parameters

None

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP attempts to go online, it receives Discovery Response packets from ACs and discover an available AC. A bogus AC may maliciously send a Discovery Response packet to the AP, causing the AP to go online on the bogus AC.

After the AC authentication function for APs is enabled, an AP initiates DTLS authentication to the AC before establishing a CAPWAP tunnel with it. The AP then uses the DTLS PSK or initial certificate to authenticate the AC. The CAPWAP tunnel can be established only after the authentication succeeds.

Precautions

After the configuration is delivered, restart the APs to make the configuration take effect.

To enable or disable the AC authentication function for APs, run the **capwap dtls server-auth disable** and **commit** commands in the AP provisioning view to deliver the configuration.

Example

Restore the default state of the AC authentication function for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] undo capwap dtls server-auth
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and may cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.195 undo capwap dtls server-auth cn (AP view)

Function

The **undo capwap dtls server-auth cn** command restores the default CN field used by APs to verify an AC's certificate.

By default, no CN field is specified for APs to verify an AC's certificate.

Format

undo capwap dtls server-auth cn

Parameters

None

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to clear the configured CN field used by APs to verify an AC's certificate. Then APs do not verify the CN field of an AC's certificate.

Precautions

After the configuration is delivered, restart the APs to make the configuration take effect.

To configure the CN field used by APs to verify an AC's certificate, run the **capwap dtls server-auth cn** *cn-string* and **commit** commands in the AP provisioning view to deliver the configuration.

Example

Restore the default CN field used by APs to verify an AC's certificate.

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



```
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] undo capwap dtls server-auth cn
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and may cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.196 unicast-suppression auto-detect (AP system profile view)

Function

The **unicast-suppression auto-detect** command configures the rate limit for unknown unicast packets during intelligent flow control.

The **undo unicast-suppression auto-detect** command restores the default rate limit for unknown unicast packets during intelligent flow control.

By default, the rate limit for unknown unicast packets is 128 pps.

Format

unicast-suppression auto-detect packets *packets*

undo unicast-suppression auto-detect

Parameters

Parameter	Description	Value
packets *packets*	Specifies the rate limit for unknown unicast packets.	The value is an integer that ranges from 64 to 1024, in pps.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When there are a large number of broadcast, multicast, and unknown unicast packets, the CPU becomes busy processing these packets and the buffer of the packet for receiving incoming packets is occupied. When the buffer decreases to the specified threshold, the device automatically rate-limits the broadcast, multicast, and unknown unicast packets. You can run this command to specify the rate limit for intelligent flow control as required. Rate limiting takes effect only for incoming traffic.

Example

Set the rate limit for unknown unicast packets during intelligent flow control to 300 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] unicast-suppression auto-detect packets 300
```

11.2.197 usb enable (AP system profile view)

Function

The **usb enable** command enables the USB function on an AP.

The **undo usb enable** command disables the USB function on an AP.

By default, the USB function on an AP is disabled.

NOTE

The operations of enabling and disabling the USB function are supported only by the following models:

- AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 9700D-M, AirEngine 5760-22WD
- AirEngine 8761-X1, AirEngine 6761-21, AirEngine 6761-21E, AirEngine 6761-21T, AirEngine 6761S-21, AirEngine 6761S-21T, AirEngine 6761-22T, AirEngine 5761-21, AirEngine 5761S-21, AirEngine 5761-11, AirEngine 5761S-11, AirEngine 5761-11W, AirEngine 5761S-11W, AirEngine 5761-11WD, AirEngine 5761-12, AirEngine 5761-12W, AirEngine 5761S-12, AirEngine 5761S-13
- AirEngine 5762-13W, AirEngine 5762-15HW, AirEngine 5762S-13W, AirEngine 5762-16W, AirEngine 5762-17W
- AirEngine 8771-X1T

For the AirEngine 5762-15HW and AirEngine 8761-X1, the USB power can only be set to 2.5 W.

Format

usb enable [**5w** | **9w**]

undo usb enable

Parameters

Parameter	Description	Value
5w	Sets the USB power to 5 W. If **5w** or **9w** is not specified, the USB power is 2.5 W.	-
9w	Sets the USB power to 9 W. If **5w** or **9w** is not specified, the USB power is 2.5 W.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use functions of the USB interface on an AP, run the **usb enable** command to enable the USB function. When the USB function is enabled, the power consumption of the AP will increase, which may affect other functions. You are advised to run the **undo usb enable** command to disable the USB function after using it.

Precautions

The USB and other functions of an AP may be restricted at different power supply levels:

- The USB function is unavailable at specific power supply levels.
- When the USB function is available and enabled, other functions (such as the IoT card, number of spatial streams, and transmit power) may be affected differently depending on power supply levels. The affected AP functions are restored after the USB function is disabled.

For details about the restrictions, do as follows: Visit **Info-Finder**, select a product series, and view hardware specifications in the hardware center. You can check the power supply downgrade limits at different power supply levels.

Example

Enable the USB function in the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] usb enable
Warning: When the USB function is enabled, the AP power consumption increases, which may affect the number of service flows and transmit power over the air interface. Continue? [Y/N]: y
```

11.2.198 user-interface vty acl

Function

The **user-interface vty acl** command uses an ACL to restrict login rights of users on a terminal.

The **undo user-interface vty acl** command cancels the configuration.

By default, login rights are not restricted.

Format

user-interface vty *ui-number* **acl** [**ipv6**] *acl-number* { **inbound** | **outbound** }

undo user-interface vty *ui-number* **acl** [**ipv6**] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
vty *ui-number*	Specifies the VTY user interface number.	The value is an integer that ranges from 0 to 4.
ipv6	Indicates an ACL6 number.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 3000 to 3031.
inbound	Restricts users with an address or within an address segment to log in to the device.	-
outbound	Restricts users who have logged in to the device from logging in to other devices.	-

Views

AP system profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command restricts the login rights of a user interface based on the source IP address, destination IP address, source port, or destination port. You can use this command to permit or deny access to a destination or from a source.

Prerequisites

Before running this command, run the **acl (system view)** in the system view and run the **rule (basic ACL view)** or **rule (advanced ACL view)** command to configure an ACL.

If no rule is configured, login rights on the user interface are not restricted when the **acl** command is executed.

Precautions

After the configurations of the ACL take effect, all users on the user interface are restricted by the ACL.

You can configure all of the following ACL types: IPv4 inbound, IPv4 outbound, IPv6 inbound, and IPv6 outbound on a user interface. Only one ACL of each type can be configured on a user interface, and only the latest configuration of an ACL takes effect.

Example

Restrict the Telnet login rights on user interface VTY 0.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule deny tcp source any destination-port eq telnet
[HUAWEI-acl-adv-3001] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] user-interface vty 0 acl 3001 outbound
```

11.2.199 user-interface vty idle-timeout

Function

The **user-interface vty idle-timeout** command sets the timeout period for disconnection from a user interface.

The **undo user-interface vty idle-timeout** command restores the default timeout period.

By default, the timeout period is 5 minutes.

Format

user-interface vty *ui-number* **idle-timeout** *minutes* [*seconds*]

undo user-interface vty *ui-number* **idle-timeout**

Parameters

Parameter	Description	Value
ui-number	Specifies the VTY user interface number.	The value is an integer that ranges from 0 to 4.
minutes	Specifies the idle timeout period, in minutes.	The value is an integer that ranges from 0 to 35791, in minutes.
seconds	Specifies the idle timeout period, in seconds.	The value is an integer that ranges from 0 to 59, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user logs in to the device and does not perform an operation, the user interface is occupied unnecessarily. You can run the **user-interface vty idle-timeout** command to disconnect the user's terminal from the device.

Precautions

If the parameters *minutes* and *seconds* are both set to **0**, the VTY timeout disconnection function is disabled.

Example

Set the timeout period to 1 minute and 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] user-interface vty 0 idle-timeout 1 30
```

11.2.200 user-interface vty screen-length

Function

The **user-interface vty screen-length** command sets the number of lines on each terminal screen after you run a command.

The **undo user-interface vty screen-length** command restores the default configuration.

By default, the number of lines to be displayed on a terminal screen is 24.

Format

user-interface vty *ui-number* **screen-length** *screen-length*

undo user-interface vty *ui-number* **screen-length**

Parameters

Parameter	Description	Value
ui-number	Specifies the VTY user interface number.	The value is an integer that ranges from 0 to 4.
screen-length	Specifies the number of lines displayed on a terminal screen.	The value is an integer that ranges from 0 to 512. The value **0** indicates that all command output is displayed on one screen.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If you run a command and its output is displayed in more lines than you can see on one screen, you can set a small number of lines displayed on each screen.

In most cases, you do not need to change the number of lines displayed on each screen. Setting the number of lines to 0 is not recommended. The configuration takes effect after you log in to the system again.

Example

Set the number of lines on each screen of the terminal to 30.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] user-interface vty 0 screen-length 30
```

11.2.201 user-isolate (AP wired port profile view)

Function

The **user-isolate** command enables user isolation on an AP's wired interface.

The **undo user-isolate** command disables user isolation on an AP's wired interface.

By default, user isolation is disabled on an AP's wired interface.

Format

user-isolate { **all** | **l2** }

undo user-isolate

Parameters

Parameter	Description	Value
all	Enables Layer 2 and Layer 3 user isolation.	-
l2	Enables Layer 2 user isolation.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The user isolation function prevents users on the same wired interface from communicating with each other. All user traffic on the wired interface is forwarded by the gateway. Therefore, this function ensures communication security on wired interfaces and allows uniform charging for users.

Precautions

Eth-Trunk member interfaces do not support the user isolation function.

This function is supported only when the AP's wired interface works in endpoint or middle mode.

Example

Set the working mode of the AP's wired interface GE0 to **endpoint** and enable Layer 2 user isolation on GE0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode configuration will cause the AP to go out of management . This fault can be recovered only by modifying the configuration on the AP. Continue? [Y/N]:y
[HUAWEI-wlan-wired-port-wired] user-isolate l2
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.202 vlan pvid (AP wired port profile view)

Function

The **vlan pvid** command sets the PVID for an AP's wired interface.

The **undo vlan pvid** command deletes the PVID of an AP's wired interface.

By default, the PVID of an AP's wired interface is 1.

Format

vlan pvid *vlan-id*

undo vlan pvid

Parameters

Parameter	Description	Value
vlan-id	Specifies the PVID of an AP's wired interface.	The value is an integer that ranges from 1 to 4094.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

APs on a WLAN WDS network only process tagged packets.

When receiving an untagged packet from a peer device, an AP's wired interface adds a VLAN tag to the packet. After the PVID is configured on the wired interface, the interface adds the PVID to all the received untagged packets.

Precautions

Eth-Trunk member interfaces do not support PVID setting.

The PVID can be configured in different modes for an AP's wired interface.

- When the AP's wired interface works in root mode, the PVID can be directly configured.
- When the AP's wired interface works in endpoint mode, the PVID can be directly configured.
- When the AP's wired interface works in middle mode, the PVID cannot be configured.

Example

Set the working mode of the AP's wired interface GE0 to **endpoint** and set the PVID of GE0 to VLAN 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode configuration will cause the AP to go out of management . This fault can be recovered only by modifying the configuration on the AP. Continue? [Y/N]:y
[HUAWEI-wlan-wired-port-wired] vlan pvid 1
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```


11.2.203 vlan (AP wired port profile view)

Function

The **vlan** command configures the VLAN to which an AP's wired interface belongs.

The **undo vlan** command deletes the VLAN to which an AP's wired interface belongs.

By default, when an AP's wired interface works in **root** mode, it joins VLAN 1 in untagged mode and joins all other VLANs in tagged mode. When the interface does not work in **root** mode, it joins VLAN 1 only in untagged mode.

NOTE

An AP's wired interface can be added to a maximum of 256 VLANs.

Format

vlan { **tagged** | **untagged** } { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan { **all** | *vlan-id1* [**to** *vlan-id2*] &<1-10> }

Parameters

Parameter	Description	Value
tagged	Adds a wired interface to a VLAN in tagged mode.	-
untagged	Adds a wired interface to a VLAN in untagged mode.	-

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the ID of the VLAN to which the wired interface belongs. • *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 wired interface is added to the VLAN specified by *vlan-id1*. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	• The value of *vlan-id1* is an integer that ranges from 1 to 4094. • The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes all VLANs to which the AP's wired interface belongs.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a wired interface connects to a PC or Layer 2 network, the interface is equivalent to a hybrid interface on a switch, and can forward the packets with multiple VLAN tags.

After the **vlan tagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command is executed to add the wired interface to one or more VLANs in tagged mode, the interface does not remove VLAN tags from the packets it forwarded.

After the **vlan untagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command is executed to add the wired interface to one or more VLANs in untagged mode, the interface removes VLAN tags from the packets it forwarded.

Precautions

After you run the **management-vlan** *vlan-id* command to enable CAPWAP packets to carry the management VLAN tag, ensure that the AP's uplink wired interface is added to the management VLAN in tagged mode. By default, the VLAN ID meets the requirement. To change the VLAN ID, run the **vlan tagged** *vlan-id* command.

After the **management-vlan** *vlan-id* command is executed to configure AP's wired interfaces to send CAPWAP packets carrying the management VLAN tag (not VLAN 1), the interfaces working in **root** mode are added to VLAN 1 in tagged mode, which cannot be changed.

Eth-Trunk member interfaces cannot be added to VLANs.

Example

Set the working mode of the AP wired interface GE0 to **endpoint** and add GE0 to VLANs 3, 4, 5, and 10 in **tagged** mode and to VLANs 12, 13, 14, and 20 in **untagged** mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode configuration will cause the AP to go out of management . This fault can be recovered only by modifying the configuration on the AP.
Continue? [Y/N]:y
[HUAWEI-wlan-wired-port-wired] vlan tagged 3 to 5 10
[HUAWEI-wlan-wired-port-wired] vlan untagged 12 to 14 20
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.204 wifi-light

Function

The **wifi-light** command specifies the parameter reflected by the blinking frequency of the Wireless indicators on an AP. When a Wireless indicator blinks fast, the signal strength is strong or the service traffic volume is high.

The **undo wifi-light** command restores the default parameter reflected by the blinking frequency of the Wireless indicators on an AP.

By default,

- If the Mesh function is enabled on the AP, the blinking frequency of the Wireless indicators reflects the weakest signal strength of all neighboring APs.
- If WDS is enabled on an AP, the blinking frequency of the Wireless indicators reflects the strength of signals received from a WDS AP.
  - If the AP works in leaf mode, the blinking frequency of the Wireless indicators reflects the strength of signals received from a middle AP.
  - If the AP works in middle mode, the blinking frequency of the Wireless indicators reflects the strength of signals received from a root AP.

  - If the AP works in root mode, the blinking frequency of the Wireless indicators reflects the weakest signal strength of middle APs.
- If the WDS and Mesh functions are disabled on an AP, the blinking frequency of the Wireless indicators reflects the service traffic volume on the radio.

NOTE

Only APs with wireless indicators support this command. For details about whether an AP has wireless indicators, see the indicator description of the corresponding AP model.

Format

wifi-light { **signal-strength** | **traffic** }

undo wifi-light

Parameters

Parameter	Description	Value
signal-strength	Sets the parameter reflected by the blinking frequency of the Wireless indicators on an AP to signal strength. When a Wireless indicator blinks fast, the signal strength is strong.	-
traffic	Sets the parameter reflected by the blinking frequency of the Wireless indicators on an AP to service traffic volume. When a Wireless indicator blinks fast, the service traffic volume is high.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During installation and commissioning of APs that have the WDS or Mesh function enabled, you need to adjust WDS or Mesh AP locations and antenna directions to obtain strong signals. If the blinking frequency of the Wireless indicators shows the signal strength, onsite installation personnel can know the signal strength in real time. The **wifi-light** command allows you to specify the parameter reflected by the blinking frequency of the Wireless indicators. For example, you can specify the parameter to signal strength during installation and service traffic volume after installation.

Precautions

This command takes effect only when the AP has the WDS or Mesh function enabled. If the WDS and Mesh functions are disabled on the AP, the Wireless indicators always show service traffic volume.

Example

Set the parameter reflected by the blinking frequency of the Wireless indicators on an AP to service traffic volume.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio-profile1
[HUAWEI-wlan-radio-2g-prof-radio-profile1] wifi-light traffic
```

11.2.205 wired-port-profile (WLAN view)

Function

The **wired-port-profile** command creates an AP wired port profile and displays the AP wired port profile view, or displays the view of an existing AP wired port profile.

The **undo wired-port-profile** command deletes an AP wired port profile.

By default, the system provides the AP wired port profile **default**.

Format

wired-port-profile name *profile-name*

undo wired-port-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an AP wired port profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all AP wired port profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP wired port profile provides convenience for AP wired interface management and configuration. You can configure AP wired interface parameters in an AP wired port profile to manage APs.

Follow-up Procedure

Run the **wired-port-profile (AP group view and AP view)** command to bind the AP wired port profile to an AP or AP group so that the AP wired port profile can take effect.

Precautions

- The AP wired port profile **default** cannot be deleted.
- The AP wired port profile referenced by an AP or AP group cannot be deleted. To delete the AP wired port profile, unbind it from the AP or AP group first.

Example

Create the AP wired port profile **wired-port1** and display the AP wired port profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1]
```

11.2.206 wired-port-profile (AP group view and AP view)

Function

The **wired-port-profile** command binds an AP wired port profile to an AP or AP group.

The **undo wired-port-profile** command unbinds an AP wired port profile from an AP or AP group.

By default, the AP wired port profile **default** is bound to an AP group, but no AP wired port profile is bound to an AP.

Format

wired-port-profile *profile-name interface-type interface-number*

undo wired-port-profile *interface-type interface-number*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port profile.	The AP wired port profile must exist.
interface-type interface-number	Specifies the type and number of an AP's wired interface.	-

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an AP wired port profile using the **wired-port-profile (WLAN view)** command, bind it to an AP or AP group so that the AP wired port profile can take effect.

Precautions

- After an AP wired port profile is bound to an AP or AP group, parameter settings in the AP wired port profile apply to specified interfaces of all APs using the AP wired port profile.
- For APs with cards, the AP wired port profile can take effect only after being applied in the card view. For detailed configuration, see **wired-port-profile (IoT card interface view)**.

Example

Create the AP wired port profile **wired-port1** and bind it to GE0 on APs in AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] wired-port-profile wired-port1 gigabitethernet 0
```

11.3 Cloud-based Management Configuration Commands

11.3.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.3.2 ap manage-mode force-tradition

Function

The **ap manage-mode force-tradition** command sets the AP management mode to the local AC mode.

The **undo ap manage-mode force-tradition** command sets the AP management mode to the same as that on the switch. That is, if the NETCONF mode is enabled on the switch, the AP is managed by iMaster NCE-Campus; if the NETCONF mode is disabled on the switch, the AP is locally managed by the switch.

By default, the AP management mode is the same as that on the switch.

Format

ap manage-mode force-tradition

undo ap manage-mode force-tradition

Parameters

None

Views

NETCONF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After NETCONF is enabled on a switch (with the native AC function enabled), Fit APs are managed by iMaster NCE-Campus by default. AP entries delivered by iMaster NCE-Campus take effect, and cloud management license resources are consumed. Additionally, the switch no longer supports the commands listed in **Table 11-130**. To locally manage APs (using local AP entries and local license resources), run the **ap manage-mode force-tradition** command to set the AP management mode to the local AC mode. Then, the commands become available on the switch.

Precautions

When a Fit AP is managed by iMaster NCE-Campus, running the **ap manage-mode force-tradition** command on the switch will disconnect the Fit AP from iMaster NCE-Campus. In this case, deleting the entry of this AP on iMaster NCE-

Campus will delete the corresponding AP entry on the switch synchronously. To enable the AP to go online on the switch, you need to manually confirm the AP by running the **ap-confirm** { **all** | **mac** *ap-mac* | **sn** *ap-sn* } command on the switch.

Table 11-130 Commands that are not supported by the switch in NETCONF mode

Command	Function Description
ap auth-mode { **mac-auth** | **no-auth** | **sn-auth** } **undo ap auth-mode**	Configures the AP authentication mode. For a switch in NETCONF mode, the AP authentication mode is SN authentication.
ap blacklist mac *ap-mac1* [**to** *ap-mac2*] **undo ap blacklist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **all** }	Adds APs to an AP blacklist, or deletes APs from an AP blacklist.
ap modify *ap-id* **mac** *ap-mac*	Modifies the MAC address of an AP.
ap whitelist { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] } **undo ap whitelist** { **mac** { *ap-mac1* [**to** *ap-mac2*] | **all** } | **sn** { *ap-sn1* [**to** *ap-sn2*] | **all** } }	Adds APs to an AP whitelist, or deletes APs from an AP whitelist.
ap-confirm { **all** | **mac** *ap-mac* | **sn** *ap-sn* }	Confirms unauthorized APs and allows them to go online.
ap-name *ap-name*	Configures an AP name.
ap-rename { **ap-name** *name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* } **new-name** *ap-new-name*	Changes the name of an AP.

Example

Set the AP management mode to the local AC mode.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] ap manage-mode force-tradition
```

11.3.3 ap up-report-cloud

Function

The **ap up-report-cloud** command reports the AP status to iMaster NCE-Campus.

Format

ap up-report-cloud { **all** | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Specifies all APs.	-
ap-id *ap-id*	Specifies an AP ID.	The AP ID must already exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

In a cloud AC scenario, if the AP status on iMaster NCE-Campus is different from that on the AC, you can run this command on the AC to report the AP status to iMaster NCE-Campus again to ensure that the AP status is correctly displayed.

Example

Report the status of AP with the ID of 5 to iMaster NCE-Campus.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap up-report-cloud ap-id 5
```

11.3.4 ap-id synchronize

Function

The **ap-id synchronize** command synchronizes newly added AP IDs to the SDN controller.

Format

ap-id synchronize

Parameters

None

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AC uses NETCONF to register with the SDN controller, if AP capacity expansion is required, you can add AP IDs offline to the AC and then run this command to synchronize the newly added AP IDs to the SDN controller.

Example

Synchronize newly added AP IDs to the SDN controller.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] ap-id synchronize
```

11.3.5 display cloud license

Function

The **display cloud license** command displays license resources delivered by iMaster NCE-Campus to the AC.

Format

display cloud license

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display cloud license** command displays license resources delivered by iMaster NCE-Campus to the AC.

In CloudCampus Solution, licenses are used to control the number of APs that can be managed by iMaster NCE-Campus and the service duration. Users need to purchase licenses from service providers and import the licenses to iMaster NCE-Campus. After an AC goes online, iMaster NCE-Campus converts license resources into the expiration date and delivers the date to the AC. If the AC is out of management by iMaster NCE-Campus, AP entries and license resources on the AC are still available within the grace period of 90 days, and the AC can still manage and configure Fit APs.

You can query only the expiration date of the license on the AC. To query the number of license resources, log in to iMaster NCE-Campus to check license information.

Only devices in NETCONF mode support this command.

Example

Display license resources delivered by iMaster NCE-Campus to the AC.

```
<HUAWEI> display cloud license
--------------------------------------------------------------------------------
License type              Expire time
--------------------------------------------------------------------------------
Indoor AP                 -
Outdoor AP                 2020-12-11
Indoor AP-S               2020-12-11
Outdoor AP-S               2020-12-11
Indoor AP-EC              -
Outdoor AP-EC              2020-12-11
Common AP                 -
Indoor Wi-Fi 6 AP          2020-12-11
Outdoor Wi-Fi 6 AP         2020-12-11
Wi-Fi 7 AP                2020-12-11
Agile distributed AP       2020-12-11
--------------------------------------------------------------------------------
Total: 11
```

Table 11-131 Description of the **display cloud license** command output

Item	Description
License type	License type. • Indoor AP: license for indoor APs • Outdoor AP: license for outdoor APs • Indoor AP-S: license for indoor APs (AP models ending with -S) • Outdoor AP-S: license for outdoor APs (AP models ending with -S) • Indoor AP-EC: license for indoor APs (AP models ending with EC) • Outdoor AP-EC: license for outdoor APs (AP models ending with EC) • Common AP: common license for ACs and APs (trial license) • Indoor Wi-Fi 6 AP: license for indoor APs (Wi-Fi 6 series indoor APs) • Outdoor Wi-Fi 6 AP: license for outdoor APs (Wi-Fi 6 series outdoor APs) • Wi-Fi 7 AP: license for Wi-Fi 7 series APs • Agile distributed AP: license for central APs and distributed APs

Item	Description
Expire time	License expiration date. The value - indicates no license resource. **NOTE** • If license resources for **Common AP** and a series of APs both expire or do not exist, all APs of this series cannot go online on the AC.

11.4 WLAN Radio Resource Management Configuration Commands

11.4.1 Command Support

- WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.4.2 agc-threshold

Function

The **agc-threshold** command sets the AGC threshold for APs.

The **undo agc-threshold** command restores the default AGC threshold for APs.

By default, the AGC threshold is not configured.

Format

agc-threshold high *high-threshold*

undo agc-threshold high

Parameters

Parameter	Description	Value
high	Configures the upper AGC threshold or restores the default value.	-
high-threshold	Specifies the upper AGC threshold.	The value is an integer that ranges from –128 to –40, in dBm.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AGC threshold is used to adjust the receiver sensitivity of packets received over the air interface.

In high-density office or stadium scenarios, you can set the AGC threshold to reduce co-channel interference in some areas. The recommended value is -82 dBm. In other scenarios, you are advised to retain the default value or set this parameter under the guidance of technical support personnel.

Precautions

The anti-interference algorithm dynamically adjusts the CCA and AGC thresholds of APs. If the CCA or AGC threshold is manually configured when the anti-interference algorithm is enabled, the manually configured threshold takes effect.

Before configuring the AGC threshold, ensure that the uplink signal strength of all STAs associated with the radio is 3 dB higher than the AGC threshold. For example, if the lowest uplink signal strength of associated STAs is -83 dBm, you are advised to set the AGC threshold to -86 dBm.

Example

Set the upper AGC threshold to –70 dBm in the 2G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] agc-threshold high -70
Warning: This parameter will affect the uplink access coverage or user access.
It is recommended that the configuration be modified under the guidance of profe
ssional technical personnel. The manually configured AGC threshold takes precede
nce over the anti-interference algorithm. If the anti-interference function is e
nabled, dynamic AGC adjustment does not take effect and the manually configured
AGC threshold takes effect. Continue? [Y/N]:y
```

11.4.3 amc-policy

Function

The **amc-policy** command configures an adaptive modulation and coding (AMC) algorithm for a radio.

The **undo amc-policy** command restores the default AMC algorithm for a radio.

By default, a radio uses the AMC algorithm **auto-balance**.

NOTE

This command does not take effect for the following APs:

- AirEngine X77X
- AirEngine X761
- AirEngine X762
- Wi-Fi 5 series APs

Format

amc-policy { **auto-balance** | **high-stability** | **high-throughput** }

undo amc-policy

Parameters

Parameter	Description	Value
auto-balance	Indicates the **auto-balance** algorithm.	-
high-stability	Indicates the **high-stability** algorithm.	-
high-throughput	Indicates the **high-throughput** algorithm.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Radios need to adjust the AMC algorithm according to different scenarios to deliver the optimal user experience. Three AMC algorithms are available:

- **auto-balance**: applicable to most wireless scenarios
- **high-stability**: applicable to scenarios with continuous interference.
- **high-throughput**: applicable to scenarios with good wireless signals and non-continuous interference.

Example

Set the AMC algorithm of a radio to **high-stability**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] amc-policy high-stability
```


11.4.4 air-scan-profile

Function

The **air-scan-profile** command creates an air scan profile and displays the air scan profile view.

The **undo air-scan-profile** command deletes an air scan profile.

By default, the system provides the air scan profile **default**. You can run the **display air-scan-profile** command to view configuration of the air scan profile **default**.

Format

air-scan-profile name *profile-name*

undo air-scan-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an air scan profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all air scan profiles.	The air scan profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an air scan profile is created using the **air-scan-profile** command and bound to a radio profile, and scanning functions are enabled, such as radio calibration,

smart roaming, spectrum analysis, WLAN location, and WIDS, the AP periodically scans surrounding radio signals and reports the collected information to an AC or a server. The information is used for radio calibration, smart roaming spectrum analysis, WLAN location, or WIDS data analysis.

Follow-up Procedure

Run the **air-scan-profile (radio profile view)** command to bind the air scan profile to a 2G radio profile or 5G radio profile so that the air scan profile can take effect.

Example

Create the air scan profile **air-scan01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name air-scan01
[HUAWEI-wlan-air-scan-prof-air-scan01]
```

11.4.5 air-scan-profile (radio profile view)

Function

The **air-scan-profile** command binds an air scan profile to a radio profile.

The **undo air-scan-profile** command unbinds an air scan profile from a radio profile.

By default, the air scan profile **default** is bound to a radio profile.

Format

air-scan-profile *profile-name*

undo air-scan-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an air scan profile.	The air scan profile name must already exist.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After you create an air scan profile using the **air-scan-profile** command, bind it to a radio profile so that the air scan profile can take effect.

Example

Bind the air scan profile **air-scan01** to the radio profile **office01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name air-scan01
[HUAWEI-wlan-air-scan-prof-air-scan01] quit
[HUAWEI-wlan-view] radio-2g-profile name office01
[HUAWEI-wlan-radio-2g-prof-office01] air-scan-profile air-scan01
```

11.4.6 antenna-mode

Function

The **antenna-mode** command configures the antenna mode for an AP.

The **undo antenna-mode** command restores the default antenna mode of an AP.

By default, the automatic antenna mode is used on an AP.

Format

antenna-mode { **omnidirection** | **direction** | **auto** }

undo antenna-mode

Parameters

Parameter	Description	Value
omnidirection	Indicates the omnidirectional antenna mode.	-
direction	Indicates the directional antenna mode.	-
auto	Indicates the automatic antenna mode.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

For APs with built-in Dynamic-Zoom Smart Antennas, 5 GHz radios can work in omnidirectional or directional antenna mode to meet the requirements of common coverage scenarios (AP spacing > 12 m) or indoor high-density coverage scenarios (AP spacing: 10 m to 12 m). This function takes effect only for 5 GHz radios but not for APs without built-in Dynamic-Zoom Smart Antennas.

Built-in dynamic-zoom smart antennas are supported only by the AirEngine 6761-21, AirEngine 8771-X1T, and AirEngine 6761S-21.

The omnidirectional antenna mode is used for omnidirectional coverage, enabling a single AP to provide wider coverage. The directional antenna mode is used for indoor high-density deployment, allowing more APs to be deployed in an area and therefore providing a larger network capacity. In automatic antenna mode, the directional or omnidirectional mode is automatically selected based on the radio calibration algorithm. In actual project delivery, select a proper antenna mode based on the deployment scenario:

- Configure the directional antenna mode in indoor high-density coverage scenarios.
- Configure the omnidirectional antenna mode in common coverage scenarios.

NOTE

For APs with built-in Dynamic-Zoom Smart Antennas, if the directional antenna mode is used, the edge RSSI decreases by 3 dB. In this case, to ensure network coverage, run the **calibrate tpc threshold** *threshold* command to increase the TPC coverage threshold by 3 dB.

When the distance between APs with built-in Dynamic-Zoom Smart Antennas is 10 m to 12 m, co-channel interference may occur in the following scenarios:

- If there is no obstacle between two APs: Another AP is deployed between the APs, and the directional antenna mode is configured on both the APs.
- If there are obstacles between two APs (for example, two neighboring APs are deployed on two sides of a corner): The attenuation caused by obstacles is between 15 dB and 20 dB, and the directional antenna mode is configured on either AP. In this case, the two APs cannot detect each other.

Example

Configure an AP to work in directional antenna mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] antenna-mode direction
Warning: The directional mode is recommended only for high-density scenarios. In
 other scenarios, this configuration may deteriorate AP coverage performance. If
 radio calibration is ongoing, this configuration takes effect after calibration
 is complete. Continue? [Y/N]y
```

11.4.7 anti-interference disable

Function

The **anti-interference disable** command disables the anti-interference algorithm.

The **undo anti-interference disable** command enables the anti-interference algorithm.

By default, the anti-interference algorithm is enabled.

Format

anti-interference disable

undo anti-interference disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density scenarios, the device supports the anti-interference algorithm to improve the overall throughput in the environment.

This function takes effect only for the AirEngine X760 and AirEngine 9700D-S (including matching ORUs).

Precautions

The anti-interference algorithm may cause signal deterioration or flapping. As a result, new STAs far from an AP may encounter difficulties in accessing the network.

The anti-interference algorithm dynamically adjusts the CCA and AGC thresholds of APs. If the CCA or AGC threshold is manually configured when the anti-interference algorithm is enabled, the manually configured threshold takes effect.

Example

Disable the anti-interference algorithm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] anti-interference disable
Warning: The per-packet-TPC function and AGC check function will become invalid when anti-interference function is disable. Continue? [Y/N]y
```


11.4.8 anti-interference agc-check disable

Function

The **anti-interference agc-check disable** command disables the automatic gain control (AGC) algorithm before packet transmission.

The **undo anti-interference agc-check disable** command enables the AGC algorithm before packet transmission.

By default, the AGC algorithm before packet transmission is enabled.

NOTE

This function takes effect only for AirEngine X760 series APs.

Format

anti-interference agc-check disable

undo anti-interference agc-check disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density scenarios, the device uses the AGC algorithm to detect air interface conflicts before sending packets and determines whether to send packets to the air interface, thereby improving the overall throughput.

Prerequisites

The anti-interference algorithm has been enabled.

Precautions

The anti-interference algorithm may cause signal deterioration or flapping. As a result, new STAs far from the AP may encounter difficulties in accessing the network.

Example

Disable the AGC algorithm before packet transmission.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] anti-interference agc-check disable
```

11.4.9 anti-interference per-packet-tpc disable

Function

The **anti-interference per-packet-tpc disable** command disables the per-packet power adjustment function.

The **undo anti-interference per-packet-tpc disable** command enables the per-packet power adjustment function.

By default, per-packet power adjustment is enabled.

NOTE

This command takes effect only for AirEngine X760 series APs.

Format

anti-interference per-packet-tpc disable

undo anti-interference per-packet-tpc disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density scenarios, the per-packet power adjustment function can properly control the transmit power of radios in an area, which reduces interference to neighboring devices while meeting wireless communication requirements.

Prerequisites

The anti-interference algorithm has been enabled.

Precautions

The anti-interference algorithm may cause signal deterioration or flapping. As a result, new STAs far from the AP may encounter difficulties in accessing the network.

Example

Disable the per-packet power adjustment function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] anti-interference per-packet-tpc disable
```

11.4.10 band-steer balance gap-threshold

Function

The **band-steer balance gap-threshold** command sets the percentage threshold for access STAs on 5 GHz radios during band steering.

The **undo band-steer balance gap-threshold** command restores the default percentage threshold for access STAs on 5 GHz radios during band steering.

By default, the percentage threshold for access STAs on 5 GHz radios during band steering is 90%.

Format

band-steer balance gap-threshold *gap-threshold*

undo band-steer balance gap-threshold

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold*	Specifies the percentage threshold for access STAs on 5 GHz radios during band steering.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

After the band steering function is configured on a multi-radio AP, the AP instructs STAs that support multiple frequency bands to preferentially connect to a 5 GHz radio.

When a STA requests to connect to an AP radio, the AP enabled with band steering will collect statistics about access STAs on each radio.

1. If the number of access STAs on the AP does not exceed the start threshold configured using the **band-steer balance start-threshold** command, the STA can preferentially associate with the 5 GHz radio.
2. If the number of access STAs exceeds the value specified by the start threshold, the AP calculates the percentage of access STAs on the 5 GHz radio using the formula: (number of access STAs on the 5 GHz radio/total number of access STAs) x 100%. If the percentage exceeds the percentage threshold for access STAs on the 5 GHz radio configured using the **band-steer balance gap-threshold** command, the STA randomly selects a frequency band.

NOTE

In most cases, you are advised to use the default values of the start threshold for the number of access STAs and the percentage threshold for access STAs on 5 GHz radios. If the two thresholds are set low, the AP may allow STAs to freely select the access frequency band when the number of STAs on 5 GHz radios is small. As a result, the 5G-prior access mechanism does not take effect, and the 5 GHz band utilization cannot be maximized.

Example

Set the percentage threshold for access STAs on 5 GHz radios to 85% in the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer balance gap-threshold 85
```

11.4.11 band-steer balance start-threshold

Function

The **band-steer balance start-threshold** command sets the start threshold for the number of access STAs during band steering.

The **undo band-steer balance start-threshold** command restores the default start threshold for the number of access STAs during band steering.

By default, the start threshold for the number of access STAs during band steering is 100.

Format

band-steer balance start-threshold *start-threshold*

undo band-steer balance start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold*	Specifies the start threshold for the number of access STAs during band steering.	The value is an integer that ranges from 0 to 100.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

After the band steering function is configured on a multi-radio AP, the AP instructs STAs that support multiple frequency bands to preferentially connect to a 5 GHz radio.

When a STA requests to connect to an AP radio, the AP enabled with band steering will collect statistics about access STAs on each radio.

1. If the number of access STAs on the AP does not exceed the start threshold configured using the **band-steer balance start-threshold** command, the STA can preferentially associate with the 5 GHz radio.
2. If the number of access STAs exceeds the value specified by the start threshold, the AP calculates the percentage of access STAs on the 5 GHz radio using the formula: (number of access STAs on the 5 GHz radio/total number of access STAs) x 100%. If the percentage exceeds the percentage threshold for access STAs on the 5 GHz radio configured using the **band-steer balance gap-threshold** command, the STA randomly selects a frequency band.

NOTE

In most cases, you are advised to use the default values of the start threshold for the number of access STAs and the percentage threshold for access STAs on 5 GHz radios. If the two thresholds are set low, the AP may allow STAs to freely select the access frequency band when the number of STAs on 5 GHz radios is small. As a result, the 5G-prior access mechanism does not take effect, and the 5 GHz band utilization cannot be maximized.

Example

Set the start threshold for the number of access STAs during band steering to 90 in the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer balance start-threshold 90
```

11.4.12 band-steer client-band-expire

Function

The **band-steer client-band-expire** command sets the aging condition for terminal band information.

The **undo band-steer client-band-expire** command restores the default aging condition for terminal band information.

By default, band information of a terminal will be aged out under conditions that an AP has consecutively received Probe frames of the terminal more than 35 times from the same frequency band.

Format

band-steer client-band-expire *probe-counters*

undo band-steer client-band-expire

Parameters

Parameter	Description	Value
probe-counters	Sets the aging condition of terminal band information to the number of times that an AP has consecutively received Probe frames of a terminal from the same frequency band.	The value is an integer that ranges from 10 to 65535.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the band steering function is enabled on an AP, the AP records frequency band information of terminals so that the terminals can preferentially access the supported and lightly loaded frequency band.

Users may change terminals' configurations, which causes the supported frequency band of terminals to change. Therefore, the AP needs to update frequency band information of terminals in a timely manner. If the AP keeps receiving Probe frames of a terminal from a specific frequency band, and the number of receiving times exceeds a certain threshold, the AP updates the frequency band information of the terminal and considers that the terminal supports only the frequency band.

For example, the supported frequency bands of a terminal are 2.4 and 5 GHz frequency bands on an AP. If the AP only receives Probe frames of the terminal from the 2.4 GHz frequency band, and the number of times that the AP consecutively receives Probe frames from the 2.4 GHz frequency band exceeds the specified threshold, the AP considers that users change the terminal configuration and the terminal supports only the 2.4 GHz frequency band.

Precautions

If you set the aging condition to a large number of times that an AP consecutively receives Probe frames of a terminal from the same frequency band, the AP detects

terminal band change more slowly. A smaller number indicates quicker response. Set the aging condition according to the difference in the number of Probe frames sent from the two frequency bands.

Example

Configure the supported band information of the terminal named **default** to age out when the number of times that an AP consecutively receives Probe frames from a frequency band exceeds 80.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer client-band-expire 80
```

11.4.13 band-steer deny-threshold

Function

The **band-steer deny-threshold** command sets the maximum number of times an AP rejects association requests of a STA for band steering.

The **undo band-steer deny-threshold** command restores the default maximum number of times an AP rejects association requests of a STA for band steering.

By default, the maximum number of rejections is 0.

Format

band-steer deny-threshold *deny-threshold*

undo band-steer deny-threshold

Parameters

Parameter	Description	Value
deny-threshold	Specifies the maximum number of times an AP rejects association requests of a STA.	The value is an integer that ranges from 0 to 10.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

If a STA requests to associate with an AP from the 2.4 GHz frequency band but the AP steers the STA to the 5 GHz frequency band according to the band steering

algorithm, the AP will reject the association. However, after the number of rejections exceeds the maximum value specified by the **band-steer deny-threshold** command, the AP allows the STA to associate from the 2.4 GHz frequency band.

NOTE

The following APs do not suppress Probe Response frames on the 2.4 GHz radio before STA association. However, after STAs are associated with these APs, the STAs will be steered to the 5 GHz radio.

- AirEngine 9700D-S (including matching ORUs)
- AirEngine X77X
- AirEngine X76X

Example

Set the maximum number of rejections to 8.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer deny-threshold 8
```

11.4.14 band-steer disable

Function

The **band-steer disable** command disables the band steering function.

The **undo band-steer disable** command enables the band steering function.

By default, the band steering function is enabled.

Format

band-steer disable

undo band-steer disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with the 2.4 GHz frequency band, the 5 GHz frequency band has less interference and more available channels, and provides higher access capability.

Most STAs support both 5 GHz and 2.4 GHz frequency bands and usually associate with the 2.4 GHz radio by default when connecting to the Internet. To connect the STAs to the 5 GHz radio, you must manually select the 5 GHz radio. The band steering function frees you from the manual selection.

After you enable band steering for a specific SSID on the AC, the AP preferentially associates the terminals connected to the SSID with the 5 GHz frequency band. After the 5 GHz frequency band is fully loaded, the AP steers the terminals to the 2.4 GHz frequency band.

Configuration Impact

After the band steering function is enabled, it takes a long time for dual-band terminals to associate or roam. You are advised to disable band steering for delay-sensitive services.

Precautions

If both radios of an AP use the same VAP profile, the band steering function takes effect on both radios as long as the function is enabled for an SSID on one radio of the AP. For example, if band steering is enabled for the SSID **test** on the 2.4 GHz radio but not on the 5 GHz radio, the AP preferentially steers terminals associated with the SSID to the 5 GHz radio.

Single-radio devices do not support the band steering function.

Example

Disable band steering.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-wlan-vap-prof-test] band-steer disable
```

11.4.15 band-steer snr-threshold

Function

The **band-steer snr-threshold** command configures a start SNR threshold for triggering 5G-prior access.

The **undo band-steer snr-threshold** command restores the default start SNR threshold for triggering 5G-prior access.

The default start SNR threshold for triggering 5G-prior access is 20 dB.

Format

band-steer snr-threshold *snr-threshold*

undo band-steer snr-threshold

Parameters

Parameter	Description	Value
snr-threshold	Specifies a start SNR threshold for triggering 5G-prior access.	The value is an integer that ranges from 10 to 35, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **undo band-steer disable** command to enable the band steer function and the **band-steer snr-threshold** command to configure a start SNR threshold for triggering 5G-prior access. When the SNR in 5G Probe frames sent by a multi-band STA to a multi-radio AP exceeds the specified threshold, the STA connects to the 5G radio preferentially, improving user experience.

Example

Set the start SNR threshold for triggering 5G-prior access in the RRM profile **default** to 20 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer snr-threshold 20
```

11.4.16 bss-color disable

Function

The **bss-color disable** command disables the basic service set (BSS) coloring function.

The **undo bss-color disable** command enables the BSS coloring function.

By default, the BSS coloring function is enabled.

Format

bss-color disable

undo bss-color disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density scenarios, the 802.11ax protocol proposes the BSS coloring mechanism to improve system performance and channel usage efficiency. When detecting 802.11ax signals, STAs can identify the signals from the overlapping basic service set (OBSS) based on the BSS color bit or MAC address, and then determine air interface conflicts and perform interference management according to related information. The BSS coloring function enables a device to distinguish between the transmissions on the local and neighboring networks. Then, it can adaptively adjust the power and the sensitivity threshold to allow dynamic adjustment of the transmit power and the signal detection threshold to increase spatial reuse efficiency and minimize co-channel interference.

Precautions

Disabling the BSS coloring function will automatically disable the spatial reuse (SR) function.

The BSS coloring function does not take effect when the radio scanning function is enabled on an AP.

Example

Disable the BSS coloring function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] bss-color disable
Warning: The spatial reuse function will become invalid when BSS color function is disable. Continue?
[Y/N]y
```

11.4.17 btm-fail-times

Function

The **btm-fail-times** command sets the maximum number of attempts to steer STAs in BTM mode.

The **undo btm-fail-times** command restores the default maximum number of attempts to steer STAs in BTM mode.

By default, the maximum number of attempts to steer STAs in BTM mode is 5.

Format

btm-fail-times *btm-fail-times*

undo btm-fail-times

Parameters

Parameter	Description	Value
btm-fail-times	Specifies the number of attempts to steer STAs in BTM mode.	The value is an integer that ranges from 0 to 10. The value 0 indicates that the BTM mode is not used to steer STAs.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device preferentially uses the BTM mode to trigger STA steering to the target AP. Due to differences of STAs, some STAs can be successfully steered in BTM mode after multiple attempts. You can run the **btm-fail-times** command to set the maximum number of attempts to steer STAs in BTM mode. If the number of attempts exceeds the specified value, the device attempts to steer STAs in deauthentication mode.

Precautions

You are advised to retain the default value. If the success rate of STA steering in BTM mode is low, you can set a smaller value to improve the steering efficiency.

Example

Set the maximum number of attempts to steer STAs in BTM mode to 4.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] btm-fail-times 4
```


11.4.18 calibrate auto-bandwidth-select

Function

The **calibrate auto-bandwidth-select** { **enable** | **disable** } command enables or disables the dynamic bandwidth selection (DBS) function.

The **undo calibrate auto-bandwidth-select** command restores the default DBS state.

By default, the DBS function is disabled in the AP group radio view and not configured in the AP radio view. This command takes effect only for 5 GHz and 6 GHz radios.

Format

calibrate auto-bandwidth-select { **enable** | **disable** }

undo calibrate auto-bandwidth-select

Parameters

Parameter	Description	Value
enable	Enables the DBS function.	-
disable	Disables the DBS function.	-

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In non-high-density indoor scenarios, the DBS function can leverage the radio calibration mechanism to automatically select proper bandwidth, improving the overall system capacity.

Prerequisites

- Radio calibration has been enabled using the **calibrate enable** { **auto** | **manual** | **schedule time** } command.
- Automatic channel selection has been enabled using the **calibrate auto-channel-select enable** command.

Precautions

- The DBS function is valid only for 5 GHz and 6 GHz radios.
- The DBS function is applicable only to indoor APs with omnidirectional antennas. The adjustment effect cannot be ensured for indoor APs with directional antennas and outdoor APs.
- The DBS function takes effect only between Fit APs connected to the same AC but not between APs connected to different ACs.
- The DBS effect is not obvious for high-density scenarios.

To view historical records of channel, bandwidth, and transmit power changes caused by radio calibration, run the **display channel switch-record calibrate** command.

Example

Enable the DBS function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 1
[HUAWEI-wlan-group-radio-default/1] calibrate auto-bandwidth-select enable
```

11.4.19 calibrate auto-channel-select

Function

The **calibrate auto-channel-select** { **enable** | **disable** } command enables or disables automatic channel selection.

The **undo calibrate auto-channel-select** command restores the automatic channel selection state.

By default, the automatic channel selection function is enabled in the AP group radio view and not configured in the AP radio view.

Format

calibrate auto-channel-select { **enable** | **disable** }

undo calibrate auto-channel-select

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Two channel selection modes are available:

- Automatic mode (enabling automatic channel selection): An AP automatically selects a proper channel based on the WLAN radio environment, removing the need to specify channels manually.
- Fixed mode (disabling automatic channel selection): Channels must be manually specified.

The automatic mode (automatic channel selection) is recommended because you do not need to specify a channel for each radio. The fixed mode provides users with an alternative way when they want to specify channels by themselves or to avoid frequent channel adjustment (this may cause intermittent service interruption).

If an AP needs radio calibration, automatic channel selection must be enabled.

To view historical records of channel, bandwidth, and transmit power changes caused by radio calibration, run the **display channel switch-record calibrate** command.

NOTE

When automatic channel selection is enabled, the manually configured channels do not take effect to ensure that the radio works in the optimal channel environment.

Example

Disable automatic channel selection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] calibrate auto-channel-select disable
```

11.4.20 calibrate auto-txpower-select

Function

The **calibrate auto-txpower-select** { **enable** | **disable** } command enables or disables automatic transmit power selection.

The **undo calibrate auto-txpower-select** command restores the automatic transmit power selection state.

By default, the automatic transmit power selection function is enabled in the AP group radio view and not configured in the AP radio view.

Format

calibrate auto-txpower-select { **enable** | **disable** }

undo calibrate auto-txpower-select

Parameters

Parameter	Description	Value
enable	Enables the automatic transmit power selection function.	-
disable	Disables the automatic transmit power selection function.	-

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Two power selection modes are available:

- Automatic mode (enabling automatic transmit power selection): An AP automatically selects or adjusts the transmit power based on the WLAN radio environment, removing the need to specify AP power manually.
- Fixed mode (disabling automatic transmit power selection): The transmit power must be manually specified.

If an AP needs radio calibration, automatic transmit power selection must be enabled.

To view historical records of channel, bandwidth, and transmit power changes caused by radio calibration, run the **display channel switch-record calibrate** command.

Example

Disable automatic transmit power selection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] calibrate auto-txpower-select disable
```

11.4.21 calibrate enable { auto | manual | schedule time }

Function

The **calibrate enable** { **auto** | **manual** | **schedule time** } command configures the radio calibration mode.

The **undo calibrate enable** command disables radio calibration.

By default, the radio calibration mode is **auto**, the radio calibration interval is 1440 minutes, and the start time for radio calibration is 03:00:00.

Format

calibrate enable { **auto** [**interval** *interval-value* [**start-time** *start-time*]] | **manual** | **schedule time** *time-value* [**time-range** *time-range-name*] }

undo calibrate enable

Parameters

Parameter	Description	Value
auto	Sets the radio calibration mode to automatic calibration.	-
interval *interval-value*	Specifies the calibration interval in automatic radio calibration mode.	The value is an integer that ranges from 30 to 1440, in minutes. If **interval** is not specified, the radio calibration interval in auto mode is 1440 minutes.
start-time *start-time*	Specifies the start time for automatic radio calibration.	The value is in the format of hh:mm:ss. • hh: indicates the hour. The value is an integer that ranges from 0 to 23. • mm: indicates the minute. The value is an integer that ranges from 0 to 59. • ss: indicates the second. The value is an integer that ranges from 0 to 59.
manual	Sets the radio calibration mode to manual calibration.	-
schedule	Sets the radio calibration mode to scheduled calibration.	-
time *time-value*	Specifies the time for triggering the scheduled radio calibration.	The value is in the format of hh:mm:ss. • hh: indicates the hour. The value is an integer that ranges from 0 to 23. • mm: indicates the minute. The value is an integer that ranges from 0 to 59. • ss: indicates the second. The value is an integer that ranges from 0 to 59.

Parameter	Description	Value
time-range *time-range-name*	Specifies the name of a time range for scheduled radio calibration.	The specified time range must exist. You can run the **time-range** command to configure a time range. **NOTE** Ensure that the scheduled radio calibration time is within the time range specified by **time-range**. Otherwise, the scheduled radio calibration function does not take effect.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

There are three radio calibration modes:

- Automatic radio calibration mode: The device continuously monitors the wireless environment quality by scanning the air interface. If the air interface environment deteriorates (for example, high bit error rate or matching the policy of high noise floor), the device automatically triggers partial radio calibration to avoid interference. To prevent service interruption caused by radio calibration, you are advised to set the calibration start time during off-peak hours. To prevent frequent calibration, you are advised to set a proper calibration interval. In addition, the device performs global radio calibration periodically based on the specified start time and interval.
- Manual radio calibration mode: Global radio calibration is not automatically implemented by the device but manually triggered through the **calibrate manual startup** command.
- Schedule radio calibration mode: The device triggers radio calibration only at a specified time point (specified by **time**) or in a specified time range (specified by **time-range**).

The three modes cannot be configured simultaneously. You can choose any of the modes as required.

In any mode, you can run the **calibrate manual startup** command to trigger global radio calibration. In manual radio calibration mode, the device implements global radio calibration only after the **calibrate manual startup** command is executed.

NOTE

Regardless of the calibration mode, an AP triggers partial radio calibration when detecting the following situations:

- The packet retransmission rate exceeds the threshold. (You can run the **calibrate retransmission-rate-threshold** command to configure the threshold.)
- The air interface environment deteriorates. (You can run the **calibrate interference-check threshold** command in the diagnostic view to configure the threshold.)

Example

Set the radio calibration mode to manual calibration.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable manual
```

Set the radio calibration mode to scheduled calibration and set the scheduled calibration time to 20:30:00.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable schedule time 20:30:00
```

11.4.22 calibrate environment-deterioration-blacklist

Function

The **calibrate environment-deterioration-blacklist** command sets the blacklist threshold for the number of times the channel environment deteriorates.

The **undo calibrate environment-deterioration-blacklist** command restores the default blacklist threshold for the number of times the channel environment deteriorates.

By default, the blacklist threshold for the number of times the channel environment deteriorates is 16.

Format

calibrate environment-deterioration-blacklist threshold *threshold*

undo calibrate environment-deterioration-blacklist

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the blacklist threshold for the number of times the channel environment deteriorates.	The value is an integer that ranges from 1 to 48.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

When detecting that the environment of a channel deteriorates, the device generates an environment deterioration alarm and accumulates the number of environment deterioration times on the channel. If this number exceeds the threshold, the channel is added to the calibration blacklist. The device will skip this channel when performing radio calibration next time. If the number of environment deterioration times does not exceed the threshold, interference penalty is performed accordingly.

NOTE

If the number of environment deterioration times on more than half of calibration channels exceeds the threshold, the device performs interference penalty on all channels in the next calibration but does not add the channels to the blacklist.

Example

Set the blacklist threshold for the number of times the channel environment deteriorates to 20.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate environment-deterioration-blacklist threshold 20
```

11.4.23 calibrate retransmission-rate-check

Function

The **calibrate retransmission-rate-check** command configures the interval and traffic threshold for checking the retransmission rate.

The **undo calibrate retransmission-rate-check** command restores the default interval and traffic threshold for checking the retransmission rate.

The default interval and traffic threshold for checking the retransmission rate are 1 minute and 1250 kbit/s, respectively.

Format

calibrate retransmission-rate-check interval *interval* **traffic-threshold** *traffic-threshold*

undo calibrate retransmission-rate-check

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for checking the retransmission rate.	The value is an integer that ranges from 1 to 10, in minutes.
traffic-threshold *traffic-threshold*	Specifies the traffic threshold for checking the retransmission rate.	The value is an integer that ranges from 1 to 20000, in kbit/s.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **calibrate retransmission-rate-check** command to lower the sensitivity for collecting radio retransmission rate statistics. When the rate of network traffic reaches the threshold, retransmission rate check is performed at the specified interval.

Example

Set the interval and traffic threshold for checking the retransmission rate in the RRM profile **80211b** to 2 minutes and 1000 kbit/s, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name 80211b
[HUAWEI-wlan-rrm-prof-80211b] calibrate retransmission-rate-check interval 2 traffic-threshold 1000
```

11.4.24 calibrate retransmission-rate-threshold

Function

The **calibrate retransmission-rate-threshold** command sets the retransmission rate threshold.

The **undo calibrate retransmission-rate-threshold** command restores the default retransmission rate threshold.

By default, the retransmission rate threshold is 60%.

Format

calibrate retransmission-rate-threshold *retransmission-rate-threshold*

undo calibrate retransmission-rate-threshold

Parameters

Parameter	Description	Value
retransmission-rate-threshold	Specifies the retransmission rate threshold.	The value is an integer that ranges from 20 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The retransmission rate is the ratio of retransmitted packets to all packets sent by a radio.

The retransmission rate threshold determines whether the radio environment is normal. When the retransmission rate of a radio reaches the threshold, the system considers that the radio environment deteriorates. When this occurs, the system may start radio calibration or take measures to avoid signal interference.

Example

Set the retransmission rate threshold to 70% in the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate retransmission-rate-threshold 70
```

11.4.25 calibrate flexible-radio

Function

The **calibrate flexible-radio** { **auto-switch** | **auto-off** } command enables global dynamic frequency assignment (DFA) and sets the mode for processing redundant radios.

The **undo calibrate flexible-radio** command disables global DFA.

By default, global DFA is disabled.

Format

calibrate flexible-radio { **auto-switch** | **auto-off** }

undo calibrate flexible-radio

Parameters

Parameter	Description	Value
auto-switch	Automatically switches redundant 2.4 GHz radios to 5 GHz radios. If no channel is available on a 5 GHz radio or the current radio cannot be switched to a 5 GHz radio, the current radio is switched to the monitor mode.	-
auto-off	Automatically disables redundant 2.4 GHz radios.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DFA applies to scenarios where indoor APs with omnidirectional antennas are densely deployed, the 2.4 GHz frequency band has severe co-channel interference, and most STAs on the network support the 5 GHz frequency band.

DFA automatically switches or disables redundant radios.

- If an AP does not support radio switchover, you are advised to specify **auto-off** in the command to reduce co-channel interference and save energy.
- If an AP supports radio switchover, you are advised to specify **auto-switch** in the command to increase network capacity. If most redundant 2.4 GHz radios are automatically switched to the monitor mode, channel resources on the current network are properly used. In this case, you can specify **auto-off** in the command.

Prerequisites

The radio calibration function has been enabled using the **calibrate enable** { **auto** | **manual** | **schedule time** } command.

Precautions

DFA reduces the deployment density of 2.4 GHz radios and increases the transmit power of 2.4 GHz radios. To ensure the 5 GHz access ratio of STAs, keep the band steering function enabled.

When DFA is disabled, redundant radios are switched back to 2.4 GHz radios and the system automatically triggers radio calibration, which may degrade wireless service experience.

Example

Enable global DFA and set the mode for processing redundant radios to automatic switchover.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable auto
[HUAWEI-wlan-view] calibrate flexible-radio auto-switch
```

11.4.26 calibrate flexible-radio disable

Function

The **calibrate flexible-radio disable** command disables DFA of specified radios.

The **undo calibrate flexible-radio disable** command enables DFA of specified radios.

By default, the DFA function of a radio is enabled.

Format

calibrate flexible-radio disable

undo calibrate flexible-radio disable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After global DFA is enabled, you can run this command to disable DFA of a single AP radio or radios of an AP group in some areas.

Prerequisites

Global DFA has been enabled using the **calibrate flexible-radio** { **auto-switch** | **auto-off** } command.

Example

Disable DFA of radio 0 of AP 1.

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



```
[HUAWEI-wlan-view] calibrate enable auto
[HUAWEI-wlan-view] calibrate flexible-radio auto-switch
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] calibrate flexible-radio disable
```

11.4.27 calibrate flexible-radio manual-recognize

Function

The **calibrate flexible-radio manual-recognize** command triggers identification of redundant radios.

Format

calibrate flexible-radio manual-recognize

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The network administrator can run this command to manually trigger identification of redundant radios, and can enable DFA if discovering that redundant radios exist on the network.

Prerequisites

The radio calibration function has been enabled using the **calibrate enable** { **auto** | **manual** | **schedule time** } command.

Precautions

This command only triggers identification of redundant radios but does not switch or disable identified redundant radios.

Radio scanning is required for identifying redundant radios, which may degrade wireless service experience.

Follow-up Procedure

After redundant radios are identified, you can run the **display flexible-radio status** command to check the status of the redundant radios.

Example

Trigger identification of redundant radios.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable auto
[HUAWEI-wlan-view] calibrate flexible-radio manual-recognize
```

11.4.28 calibrate grouping interference-threshold

Function

The **calibrate grouping interference-threshold** command sets the interference threshold of a calibration group.

The **undo calibrate grouping interference-threshold** command restores the default interference threshold of a calibration group.

The default interference threshold of a calibration group is –127 dBm.

Format

calibrate grouping interference-threshold *threshold*

undo calibrate grouping interference-threshold

Parameters

Parameter	Description	Value
threshold	Specifies the interference threshold of a calibration group.	The value is an integer that ranges from –127 to –1, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During radio calibration, the system adds neighboring APs to the same calibration group and allocates channels to them. If there are a large number of APs in a calibration group but only a few channels are available, the same channel may be allocated to neighboring APs. In scenarios where APs are blocked by walls or deployed regularly, such as dormitories and hotels, you can set a proper RSSI interference threshold to control the number of APs in the same calibration group. This effectively reduces the probability that neighboring APs use the same

channel. If the RSSI of a neighbor working at the maximum power exceeds the threshold, the neighbor is added to the same calibration group. **In other scenarios, use the default value.**

Precautions

In typical scenarios, it is recommended that the interference threshold in a calibration group be set to –70 dBm. If severe co-channel interference exists between APs and neighboring APs, you can sample 1/10 of APs on each floor and calculate the accurate threshold so that the calibration algorithm can stagger the channels of neighboring APs. The specific calculation method is as follows:

1. Run the **display radio all** command and query the maximum power of each radio based on the **ME** field in the command output.
2. Run the **display ap neighbor** command to query information about neighboring APs of the target AP. Based on the **RSSI pathloss** field in the command output, calculate the maximum power values of the neighboring APs.
3. Sort the RSSIs of neighboring APs in descending order (for example, –58 dBm, –60 dBm, –62 dBm, –80 dBm, –84 dBm, –86 dBm, –90 dBm), and calculate the differences between RSSIs of neighboring APs (for example, 2 dB, 2 dB, 18 dB, 4 dB, 2 dB, 4 dB).
4. Find the first edge point where the RSSI difference is greater than or equal to 15 dB in descending order of neighboring APs' RSSIs. Divide the neighboring APs into two groups at the point: one group with strong detected RSSIs and the other with weak detected RSSIs.

   In the preceding example, the point where the RSSI difference is 18 dB is between the neighbors with –62 dBm and –80 dBm. Therefore, the seven neighbors of the AP are divided into two groups: a group with strong detected RSSIs (–58 dBm, –60 dBm, –62 dBm) and a group with weak detected RSSIs (–80 dBm, –84 dBm, –86 dBm, –90 dBm).
5. Calculate the average value between the minimum RSSI value of the group with strong detected RSSIs and the maximum RSSI value of the group with weak detected RSSIs. Use this average value as the RSSI threshold of the calibration group.

   In the preceding example, –62 dBm and –80 dBm are extracted from the two groups. The average value of the two values is –76 dBm, which is used as the recommended RSSI interference threshold.

NOTE

If the average threshold value calculated based on the sampled APs can meet the grouping requirements of all sampled APs, you can use this value for all APs in this scenario. Otherwise, it is recommended that different thresholds be configured for specific APs.

Example

Set the interference threshold of a calibration group to –70 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate grouping interference-threshold -70
```


11.4.29 calibrate max-tx-power

Function

The **calibrate max-tx-power** command sets the maximum transmit power that can be adjusted through radio calibration.

The **undo calibrate max-tx-power** command restores the default maximum transmit power that can be adjusted through radio calibration.

By default, the maximum transmit power that can be adjusted through radio calibration is 127 dBm.

Format

calibrate max-tx-power { *2g-power* | **radio-5g** *5g-power* | **radio-6g** *6g-power* }

undo calibrate max-tx-power [**radio-5g** | **radio-6g**]

Parameters

Parameter	Description	Value
2g-power	Specifies the maximum transmit power that can be adjusted through 2.4 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.
radio-5g *5g-power*	Specifies the maximum transmit power that can be adjusted through 5 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.
radio-6g *6g-power*	Specifies the maximum transmit power that can be adjusted through 6 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After radio calibration is enabled, an AP uses the Transmit Power Control (TPC) algorithm to calculate the transmit power to be adjusted based on detected neighbor information. If the transmit power to be adjusted calculated using the

TPC algorithm is to large, signal interference between APs may occur. You can run the **calibrate max-tx-power** command to set the maximum transmit power that can be adjusted through TPC.

Precautions

The maximum radio calibration power must be greater than or equal to the minimum radio calibration power. You can run the **calibrate min-tx-power** command to set the minimum calibration power.

You can adjust the maximum and minimum calibration power values using the **calibrate max-tx-power** and **calibrate min-tx-power** commands. The valid AP power after radio calibration is between the two values.

Example

Set the maximum transmit power that can be adjusted through 2.4 GHz radio calibration to 30 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate max-tx-power 30
```

11.4.30 calibrate min-tx-power

Function

The **calibrate min-tx-power** command sets the minimum transmit power that can be adjusted through radio calibration.

The **undo calibrate min-tx-power** command restores the default minimum transmit power that can be adjusted through radio calibration.

By default, the minimum transmit power that can be adjusted through 2.4 GHz radio calibration is 9 dBm, and that through 5 GHz or 6 GHz radio calibration is 12 dBm.

Format

calibrate min-tx-power { *2g-power* | **radio-5g** *5g-power* | **radio-6g** *6g-power* }

undo calibrate min-tx-power [**radio-5g** | **radio-6g**]

Parameters

Parameter	Description	Value
2g-power	Specifies the minimum transmit power that can be adjusted through 2.4 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.

Parameter	Description	Value
radio-5g *5g-power*	Specifies the minimum transmit power that can be adjusted through 5 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.
radio-6g *6g-power*	Specifies the minimum transmit power that can be adjusted through 6 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After radio calibration is enabled, an AP uses the Transmit Power Control (TPC) algorithm to calculate the transmit power to be adjusted based on detected neighbor information. If the transmit power calculated using the TPC algorithm is too small, radio coverage requirements may not be met. You can run the **calibrate min-tx-power** command to set the minimum transmit power that can be adjusted through TPC.

Precautions

The minimum radio calibration power must be less than or equal to the maximum radio calibration power. You can run the **calibrate max-tx-power** command to set the maximum calibration power.

You can adjust the maximum and minimum calibration power values using the **calibrate max-tx-power** and **calibrate min-tx-power** commands. The valid AP power after radio calibration is between the two values.

Example

Set the minimum transmit power that can be adjusted through 2.4 GHz radio calibration to 10 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate min-tx-power 10
```

11.4.31 calibrate manual startup

Function

The **calibrate manual startup** command manually triggers radio calibration.

Format

calibrate manual startup [{ **ap-group** *group-name* }&<1-4> | **ap-id** *ap-list*]

Parameters

Parameter	Description	Value
ap-group *group-name*	Specifies an AP group. **NOTE** A maximum of four AP groups can be specified.	The AP group must exist.
ap-id *ap-list*	Specifies AP IDs in a batch.	The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) or hyphens (-) to separate AP IDs. For example, 5,8,10-13,20 indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

To trigger radio calibration immediately, run the **calibrate enable** { **auto** | **manual** | **schedule time** } command to enable radio calibration and then run the **calibrate manual startup** command to manually trigger radio calibration.

You can select an AP group or list to implement radio calibration for specified APs.

Example

Manually trigger radio calibration.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable auto
[HUAWEI-wlan-view] calibrate manual startup
Warning: The operation may cause business interruption, Continue? [Y/N]:y
```


11.4.32 calibrate noise-floor-threshold

Function

The **calibrate noise-floor-threshold** command specifies the noise floor threshold for triggering radio calibration.

The **undo calibrate noise-floor-threshold** command restores the default noise floor threshold for triggering radio calibration.

The default noise floor threshold for triggering radio calibration is -75 dBm.

Format

calibrate noise-floor-threshold *threshold*

undo calibrate noise-floor-threshold

Parameters

Parameter	Description	Value
noise-floor-threshold *threshold*	Specifies the noise floor threshold for triggering radio calibration.	The value is an integer that ranges from -95 to 0, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The noise floor indicates the noise strength in the current environment. A high noise floor value will make noise drown out valid data, affecting user services.

The noise floor threshold for triggering radio calibration can be used to determine whether the environment noise is normal. When detecting a noise floor value higher than the threshold, an AP reports a high noise floor message to the AC. The AC then performs radio calibration to avoid channels with high noise floor values to improve user experience.

Precautions

In most cases, the default noise floor threshold is recommended. When high noise floor leads to poor user experience, you can increase the threshold based on the real-time noise floor. To check the noise floor of an AP, run the **display ap traffic statistics wireless** command.

Example

Set the noise floor threshold for triggering radio calibration to -60 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate noise-floor-threshold -60
```

11.4.33 calibrate policy

Function

The **calibrate policy** command creates a radio calibration policy.

The **undo calibrate policy** command deletes a radio calibration policy.

By default, no radio calibration policy is created.

Format

calibrate policy { **non-wifi** | **noise-floor** }

undo calibrate policy { **non-wifi** | **noise-floor** }

Parameters

Parameter	Description	Value
non-wifi	Specifies the non-Wi-Fi mode.	-
noise-floor	Specifies the noise floor mode.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Radio calibration policies are classified into:

- Non-Wi-Fi: If non-Wi-Fi devices exist on the network, the radio calibration algorithm takes interference that may be caused by them into account when radio calibration is performed next time.
- Noise floor policy: When the noise floor of APs is high due to special external interference, service experience may deteriorate. With this radio calibration policy, the device takes actions to avoid interference. When detecting that the noise floor of the current channel exceeds the threshold for three consecutive

times, an AP notifies the AC of the high noise floor. The AC then allocates another channel to the AP and does not allocate the current channel to the AP in 30 minutes.

NOTE

Partial radio calibration triggered based on the noise floor takes effect only in automatic radio calibration mode.

The non-Wi-Fi policy is only supported by APs that support spectrum analysis.

To disable rogue interference calibration, run the **calibrate reference rogue-ap-interference disable** command.

Radio calibration triggers channel changes. Some STAs may go offline and then go online again. If these STAs exist on the network, to ensure service experience, you are advised to perform radio calibration when no service is running and disable policies that frequently trigger radio calibration. You can run the **display channel switch-record calibrate** command to check policies that frequently trigger radio calibration.

The three radio calibration policies can be used together. You can run the command multiple times to configure different radio calibration policies according to service requirements.

Prerequisites

The noise floor threshold for triggering radio calibration has been specified using the **calibrate noise-floor-threshold** *threshold* command.

Example

Create a radio calibration policy in non-Wi-Fi mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate policy non-wifi
```

11.4.34 calibrate reference 3d-data

Function

The **calibrate reference 3d-data** { **enable** | **disable** } command enables or disables the 3D radio calibration function.

The **undo calibrate reference 3d-data** command restores the default state of the 3D radio calibration function.

By default, 3D radio calibration is enabled in the AP group radio view and is not configured in the AP radio view.

Format

calibrate reference 3d-data { **enable** | **disable** }

undo calibrate reference 3d-data

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Traditional radio calibration can only construct a topology between APs based on inter-AP probe data and automatically adjust the channels and transmit power of the APs. The latest calibration algorithm can construct a 3D network topology (AP-STA-AP) based on the probe data between APs and STAs during radio calibration. This helps accurately identify the topology relationship between APs (for example, APs installed at heights). In this way, the calibration effect is improved. You can run this command to enable 3D radio calibration to achieve optimization based on the analysis result of STA measurement data.

NOTE

- The 3D radio calibration function takes effect only for APs running V200R021C10 or later.
- APs running versions earlier than V200R021C10 cannot collect or report STA measurement data. Enabling the 3D radio calibration function will affect the accuracy of identification results. If these APs exist on the network, you are advised to upgrade all APs to V200R021C10 or later, or disable the 3D radio calibration function.

Example

Enable 3D radio calibration.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-ap-group1] radio 0
[HUAWEI-wlan-group-radio-ap-group1/0] calibrate reference 3d-data enable
```

11.4.35 calibrate reference data-analysis disable

Function

The **calibrate reference data-analysis disable** disables the Big Data calibration function.

The **undo calibrate reference data-analysis** command restores the default configuration.

By default, Big Data calibration is enabled.

Format

calibrate reference data-analysis disable

undo calibrate reference data-analysis

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After Big Data calibration is enabled, the device performs calculation based on the variations in interference and load according to Big Data information obtained from the iMaster NCE-CampusInsight. This function helps better avoid interference and improve network capacity. If the Big Data calibration function is disabled, radio calibration is performed based only on the locally collected data.

The Big Data calibration function takes effect only when radio calibration is enabled.

Example

Disable the Big Data calibration function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate reference data-analysis disable
```

11.4.36 calibrate reference data-analysis

Function

The **calibrate reference data-analysis disable** command disables Big Data calibration on radio interfaces of APs and AP groups.

The **calibrate reference data-analysis enable** command enables Big Data calibration on radio interfaces of APs and AP groups.

The **undo calibrate reference data-analysis** command restores the default Big Data calibration configuration on radio interfaces of APs and AP groups.

By default, Big Data calibration is disabled on radio interfaces of APs but enabled on radio interfaces in an AP group.

Format

calibrate reference data-analysis { disable | enable }

undo calibrate reference data-analysis

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

After Big Data calibration is enabled, the device performs calculation based on the variations in interference and load according to Big Data information obtained from the iMaster NCE-CampusInsight. This function helps better avoid interference and improve network capacity. If the Big Data calibration function is disabled, radio calibration is performed based only on the locally collected data.

NOTE

The Big Data calibration function takes effect on an AP only when the following configurations are performed:

- Configure the function of reporting KPIs to the Big Data analyzer.
- Enable radio calibration.
- Run the **undo calibrate reference data-analysis** command in the WLAN view to enable the global Big Data calibration function.
- Enable the Big Data calibration function on the AP. (If the Big Data calibration function is not configured on a single AP, the configuration of the AP group takes effect.)

Example

Enable Big Data calibration on radio 0 in AP group **ap-group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] radio 0
[HUAWEI-wlan-group-radio-ap-group1/0] calibrate reference data-analysis enable
```

11.4.37 calibrate reference rogue-ap-interference disable

Function

The **calibrate reference rogue-ap-interference disable** command disables rogue interference calibration so that the device performs radio calibration only based on information about authorized neighbors.

The **undo calibrate reference rogue-ap-interference disable** command enables rogue interference calibration so that the device performs radio calibration based on information about both authorized and rogue neighbors.

By default, rogue interference calibration is enabled.

Format

calibrate reference rogue-ap-interference disable

undo calibrate reference rogue-ap-interference disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Rogue neighbors often interfere with radio signals of APs. Therefore, a WLAN usually takes rogue neighbors as one of the factors for radio calibration and avoids the channels used by the rogue neighbors. If only a few channels are available, authorized APs on the same channel may be deployed too close to each other, affecting wireless network coverage. In actual delivery, if rogue interference is low (no or little interference traffic), you can run the **calibrate reference rogue-ap-interference disable** command to adjust the radio calibration policy so that the device does not consider external Wi-Fi interference from rogue neighbors during radio calibration. In this way, more channel resources are available for allocation during radio calibration.

To take non-Wi-Fi interference into account during radio calibration, run the **calibrate policy non-wifi** command.

Example

Disable rogue interference calibration so that the device performs radio calibration only based on information about authorized neighbors.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate reference rogue-ap-interference disable
```

11.4.38 calibrate sensitivity

Function

The **calibrate sensitivity** command configures the calibration sensitivity for a device.

The **undo calibrate sensitivity** command restores the default calibration sensitivity.

By default, the calibration sensitivity of the device is **medium**.

Format

calibrate sensitivity [**2.4g** | **5g** | **6g**] { **high** | **medium** | **low** | **insensitivity** | **custom-percent** *custom-percent* }

undo calibrate sensitivity [**2.4g** | **5g** | **6g**]

Parameters

Parameter	Description	Value
high	Indicates high calibration sensitivity.	-
medium	Indicates medium calibration sensitivity.	-
low	Indicates low calibration sensitivity.	-
insensitivity	Indicates calibration insensitivity.	-
custom-percent *custom-percent*	Specifies the calibration sensitivity based on the customized threshold.	The value ranges from 0 to 100, in percentage (%). A larger value indicates a lower sensitivity.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Radio calibration sensitivity is valid only in automatic radio calibration mode (enabled using the **calibrate enable auto** command). The default value is recommended.

If the percentage of radios with severe interference reaches the calibration sensitivity threshold, global channels are adjusted during radio calibration. Otherwise, the algorithm adjusts the operating channels of only radios with severe interference.

- high: equivalent to the custom threshold of 25%
- medium: equivalent to the custom threshold of 50%
- low: equivalent to the custom threshold of 75%
- insensitivity: equivalent to the custom threshold of 100%

Example

Set the calibration sensitivity to high for radios on all frequency bands.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate sensitivity high
```


11.4.39 calibrate tpc threshold

Function

The **calibrate tpc threshold** command sets the Transmit Power Control (TPC) coverage threshold.

The **undo calibrate tpc threshold** command restores the default TPC coverage threshold.

The default TPC coverage threshold is –60 dBm.

Format

calibrate tpc threshold *threshold*

undo calibrate tpc threshold

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the TPC coverage threshold.	The value is an integer that ranges from -85 to -35, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When radio calibration is enabled, the TPC coverage threshold is different depending on AP deployment scenarios because the AP deployment distance or height differs. To ensure the optimal coverage effect, adjust the TPC coverage threshold based on the actual AP deployment situations. A large threshold indicates a wider transmit power range that can be adjusted through TPC.

Example

Set the TPC coverage threshold to -70 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate tpc threshold -70
```


11.4.40 calibrate virtual-group-size

Function

The **calibrate virtual-group-size** command sets the channel calibration group size and K value.

The **undo calibrate virtual-group-size** command restores the default channel calibration group size and K value.

By default, the channel calibration group size is 50, and the K value is 70.

Format

calibrate virtual-group-size *size-value* **k-value** *k-value*

undo calibrate virtual-group-size

Parameters

Parameter	Description	Value
size-value	Sets the channel calibration group size. This parameter is an algorithm parameter. Set it under the assistance of technical support personnel.	The value is an integer that ranges from 10 to 50.
k-value *k-value*	Sets the K value. This parameter is an algorithm parameter. Set it under the assistance of technical support personnel.	The value is an integer that ranges from 20 to 100.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can set internal algorithm parameters for radio calibration to optimize radio calibration time costs and effects. Set the parameters under the assistance of technical support personnel.

Example

Set the channel calibration group size to 40 and K value to 80.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate virtual-group-size 40 k-value 80
```


11.4.41 cca-threshold

Function

The **cca-threshold** command sets the clear channel assessment (CCA) threshold for APs.

The **undo cca-threshold** command restores the default CCA threshold of APs.

By default, no CCA threshold is specified. APs use the default CCA threshold of the chip.

NOTE

The CCA threshold does not take effect for the following APs:

- AirEngine X771
- AirEngine X761
- AirEngine X762

Format

cca-threshold *cca-threshold*

undo cca-threshold

Parameters

Parameter	Description	Value
cca-threshold	Specifies the CCA threshold for APs.	The value is an integer that ranges from –85 to –40, in dBm.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CCA mechanism enables a WLAN chip to determine whether the channel is idle before transmitting signals to the air interface. If so, the chip transmits signals. If not, the chip waits until the channel is idle.

The CCA threshold is used by the WLAN chip to evaluate whether a channel is idle. If the detected Wi-Fi signal strength on the current channel exceeds the threshold, the current channel is busy. Otherwise, the current channel is idle.

When deploying a WLAN, you can set a proper CCA threshold to reduce interference of co-channel Wi-Fi signals in the surrounding environment to the current AP and improve channel reuse rate.

In high-density coverage scenarios such as a stadium, you are advised to set the CCA threshold to -75 dBm. In other scenarios, you are advised to retain the default value or set this parameter under the guidance of technical support personnel.

Precautions

The anti-interference algorithm dynamically adjusts the CCA and AGC thresholds of APs. If the CCA or AGC threshold is manually configured when the anti-interference algorithm is enabled, the manually configured threshold takes effect.

Example

Set the CCA threshold for a 2G radio to -70 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] cca-threshold -70
Warning:  This parameter will affect the uplink access coverage or user access.
It is recommended that the configuration be modified under the guidance of profe
ssional technical personnel. The manually configured CCA threshold takes precede
nce over the anti-interference algorithm. If the anti-interference function is e
nabled, dynamic CCA adjustment does not take effect and the manually configured
CCA threshold takes effect. Continue? [Y/N]:y
```

11.4.42 co-sr disable

Function

The **co-sr disable** command disables the Coordinated Spatial Reuse (CoSR) function.

The **undo co-sr disable** command enables the CoSR function.

By default, the CoSR function is enabled.

Format

co-sr disable

undo co-sr disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

On a high-density office network, you can run the **undo co-sr disable** command to enable the CoSR function to improve the overall network throughput.

The CoSR function is supported only by AirEngine X760 series APs.

Example

Disable the CoSR function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] co-sr disable
```

11.4.43 dca-channel bandwidth

Function

The **dca-channel bandwidth** command configures the calibration bandwidth.

The **undo dca-channel bandwidth** command restores the default calibration bandwidth.

By default, the calibration bandwidth value is **auto**.

Format

dca-channel 5g bandwidth { **20mhz** | **40mhz** | **80mhz** | **auto** }

dca-channel 6g bandwidth { **20mhz** | **40mhz** | **80mhz** | **160mhz** | **320mhz** | **auto** }

undo dca-channel 5g bandwidth

undo dca-channel 6g bandwidth

Parameters

Parameter	Description	Value
5g	Specifies the 5 GHz frequency band on which radio calibration is implemented.	-
6g	Specifies the 6 GHz frequency band on which radio calibration is implemented.	-

Parameter	Description	Value
20mhz | **40mhz** | **80mhz** | **160mhz** | **320mhz** | **auto**	Specifies the calibration bandwidth. If **auto** is specified and the number of channels supported by the country code is greater than or equal to 6, the device uses 40 MHz bandwidth on the 5 GHz frequency band and 80 MHz bandwidth on the 6 GHz frequency band by default during radio calibration. This achieves larger calibration bandwidth without manual configuration. If the number of available channels is less than 6, the device decreases the calibration bandwidth (from 80 MHz to 40 MHz and to 20 MHz) on the corresponding frequency band until the number of available channels is greater than or equal to 6 or the calibration bandwidth is reduced to 20 MHz.	-

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Richer spectrum resources are available on the 5 GHz and 6 GHz frequency bands, enabling APs to work on 40 MHz or larger-bandwidth channels in addition to 20 MHz channels. Larger-bandwidth channels mean higher transmission rates. However, at least three channels are required in radio calibration to achieve the optimal calibration effect. When configuring the calibration bandwidth, ensure that enough calibration channels are available for use.

You can use the **dca-channel bandwidth** command to configure the calibration bandwidth and the **dca-channel channel-set** command to configure calibration channels as prompted.

Configuration Impact

When the calibration bandwidth is changed, the device recalculates the calibration channels.

Precautions

When configuring 40 MHz or larger calibration bandwidth, check whether channels of the corresponding bandwidth exist under the country code.

Example

Set the calibration bandwidth of 5 GHz radios to 40 MHz.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name default
[HUAWEI-wlan-regulate-domain-default] dca-channel 5g bandwidth 40mhz
```

11.4.44 dca-channel channel-set

Function

The **dca-channel channel-set** command configures a calibration channel set.

The **undo dca-channel channel-set** command restores the default calibration channel set.

By default, a calibration channel set contains channels 1, 6, and 11 on 2.4 GHz radios and contains all channels supported by the corresponding country code on 5 GHz and 6 GHz radios. When configuring a calibration channel set, you can specify channels as prompted.

Format

dca-channel { **2.4g** | **5g** | **6g** } **channel-set** *channel-value*

undo dca-channel { **2.4g** | **5g** | **6g** } **channel-set**

Parameters

Parameter	Description	Value
2.4g | **5g** | **6g**	Specifies the frequency band on which radio calibration is performed. The options are as follows: • **2.4g**: Radios work on the 2.4 GHz frequency band. • **5g**: Radios work on the 5 GHz frequency band. • **6g**: Radios work on the 6 GHz frequency band.	-

Parameter	Description	Value
channel-set *channel-value*	Specifies a calibration channel set.	The value is a character string. You can select calibration channels as prompted. If you select multiple channels, use commas (,) to separate channel names.

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Richer spectrum resources are available on the 5 GHz and 6 GHz frequency bands, enabling APs to work on 40 MHz or larger-bandwidth channels in addition to 20 MHz channels. Larger-bandwidth channels mean higher transmission rates. However, at least three channels are required in radio calibration to achieve the optimal calibration effect. When configuring the calibration bandwidth, ensure that enough calibration channels are available for use.

You can run this command to specify a calibration channel set for an AP. The AP selects channels from the channel set to calibrate. This reduces the burden on the AP.

NOTE

To ensure a good calibration effect, you are advised to configure at least three calibration channels.

To prevent signal interference, ensure that adjacent APs work in non-overlapping channels. The 2.4 GHz frequency band has overlapping channels. When configuring calibration channels, you are advised to configure a non-overlapping calibration channel set containing channels 1, 6, and 11 or containing channels 1, 5, 9, and 13.

To specify a 40 MHz calibration channel, you need to specify two consecutive 20 MHz channels. To specify an 80 MHz calibration channel, you need to specify four consecutive 20 MHz channels. The combinations of 20 MHz channels making up the 40 MHz and 80 MHz channels are fixed.

You can also use the **dca-channel bandwidth** command to configure the calibration bandwidth and the **dca-channel channel-set** command to configure calibration channels as prompted.

If no calibration channel set is configured, the device probes channels based on the calibration channels corresponding to the country code.

NOTE

When configuring a calibration channel set, avoid using radar channels.

The configured channels must be supported by STAs; otherwise, the STAs cannot discover radio signals.

Channels 184, 188, 192, and 196 on the 4.9 GHz frequency band can be used for radio scanning but cannot be used for channel calibration.

If the AP has three 5 GHz radios, configure at least five calibration channels. If the AP has two 5 GHz radios, configure at least three calibration channels.

Example

Configure a calibration channel set composed of 40 MHz channels 149, 153, 157, and 161 on the 5 GHz frequency band.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name default
[HUAWEI-wlan-regulate-domain-default] dca-channel 5g bandwidth 40mhz
[HUAWEI-wlan-regulate-domain-default] dca-channel 5g channel-set 149,153,157,161
```

11.4.45 deauth-fail-times

Function

The **deauth-fail-times** command sets the maximum number of attempts to steer STAs in deauthentication mode.

The **undo deauth-fail-times** command restores the default maximum number of attempts to steer STAs in deauthentication mode.

By default, the maximum number of attempts to steer STAs in deauthentication mode is 0.

Format

deauth-fail-times *deauth-fail-times*

undo deauth-fail-times

Parameters

Parameter	Description	Value
deauth-fail-times	Specifies the maximum number of attempts to steer STAs in deauthentication mode.	The value is an integer that ranges from 0 to 5. The value 0 indicates that the deauthentication mode is not used to steer STAs.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device attempts to use the 802.11v and deauthentication modes to trigger STA steering to the target AP. Due to differences of STAs, some STAs can be successfully steered in deauthentication mode after multiple attempts. You can run the **deauth-fail-times** command to set the maximum number of attempts to steer STAs in deauthentication mode. If the number of attempts exceeds the specified value, STAs cannot be steered.

Precautions

You are advised to retain the default value. If the success rate of STA steering in deauthentication mode is low or STA services are affected, set the parameter value to 0 to disable STA steering in deauthentication mode.

Example

Set the maximum number of attempts to steer STAs in deauthentication mode to 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] deauth-fail-times 1
```

11.4.46 dfs radar-filter sensitivity

Function

The **dfs radar-filter sensitivity** command sets the sensitivity level of correction for false DFS radar detection.

The **undo dfs radar-filter sensitivity** command restores the default sensitivity level of correction for false DFS radar detection.

By default, the sensitivity level of correction for false DFS radar detection is 0.

Format

dfs radar-filter sensitivity *level*

undo dfs radar-filter sensitivity

Parameters

Parameter	Description	Value
level	Specifies the sensitivity level of correction for false DFS radar detection.	The value is an integer that ranges from 0 to 10. • Level 0: The sensitivity of correction for false DFS radar detection is moderate. • Levels 1 to 9: A larger value indicates that correction for false DFS radar detection is more sensitive. That is, DFS radar detection is less sensitive and radar signals are less likely to be detected. • Level 10: DFS radar detection is disabled.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In most cases, you are advised to retain the default sensitivity level of correction for false DFS radar detection However, some APs may frequently detect radar signals by mistake. To prevent unnecessary channel switching, you can run the **dfs radar-filter sensitivity** command to adjust the sensitivity level as required to reduce false radar detection.

If radar signals are often falsely detected, you are advised to set the sensitivity level to 5 and then adjust the value properly based on the false radar detection events. For example, if an AP often falsely detects radar signals, the sensitivity level for radar detection is high. In this case, set the sensitivity level to 5 and continuously observe the false radar detection events. If false radar detection events persist, gradually increase the sensitivity level.

Example

Set the sensitivity level of correction for false DFS radar detection to 9 in the 5G radio profile **test1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name test1
[HUAWEI-wlan-radio-5g-prof-test1] dfs radar-filter sensitivity 9
```

11.4.47 dfs recover-delay

Function

The **dfs recover-delay** command sets the delay in switching back the DFS channel.

The **undo dfs recover-delay** command restores the default delay in switching back the DFS channel.

By default, the delay in switching back the DFS channel is 0 minutes. That is, the channel is switched back to the manually planned channel when the legitimate aging time (30 minutes) expires.

Format

dfs recover-delay *delay-time*

undo dfs recover-delay

Parameters

Parameter	Description	Value
delay-time	Specifies a delay in switching back the DFS channel.	The value is an integer that ranges from 0 to 2880, in minutes.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

For an AP operating on a manually planned channel, it randomly selects a channel (calibration channel preferred) within the range defined by the country code after detecting radar signals. The AP channel will be switched back to the manually planned channel after the configured switchback delay and legitimate aging time (30 minutes). A proper delay in switching back the DFS channel will prevent frequent channel switchovers.

Example

Set the delay in switching back the DFS channel to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] dfs recover-delay 10
```

11.4.48 dfs smart-selection disable

Function

The **dfs smart-selection disable** command disables the DFS smart selection function.

The **undo dfs smart-selection disable** command enables the DFS smart selection function.

By default, the DFS smart selection function is enabled.

Format

dfs smart-selection disable

undo dfs smart-selection disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the DFS smart selection function is enabled, an AP working on the 5 GHz band detects radar signals. Upon detecting radar channels, the AP automatically switches to another channel to prevent radar interference.

When an AP switches its working channel upon detecting radar signals, it randomly selects a channel (the calibration channel preferentially) allowed by the country code. The selected channel may be the same as or adjacent to the working channel of surrounding 5 GHz radios, thereby causing severe interference and poor network access experience. By default, the DFS smart selection function is enabled so that the AP switches to a 5 GHz channel with the minimum interference, preventing interference.

After the **dfs smart-selection disable** command is executed, the DFS smart selection function is disabled, affecting user experience. Configure this function as required.

Precautions

The DFS smart selection function is valid only when the air scan is enabled.

Example

Disable DFS smart selection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] dfs smart-selection disable
Info: This function does not take effect when air scan is disabled.
```


11.4.49 display air-scan-profile

Function

The **display air-scan-profile** command displays information about air scan profiles.

Format

display air-scan-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all air scan profiles.	-
name *profile-name*	Displays information about a specified air scan profile.	The air scan profile name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display air-scan-profile** command to view information about air scan profiles.

Example

Display information about all air scan profiles.

```
<HUAWEI> display air-scan-profile all
------------------------------------------------------------
Profile name        Reference
------------------------------------------------------------
default              2
test                 1
------------------------------------------------------------
Total: 2
```

Table 11-132 Description of the **display air-scan-profile all** command output

Item	Description
Profile name	Name of an air scan profile.

Item	Description
Reference	Number of times that the air scan profile is referenced.

Display information about the air scan profile **test**.

```
<HUAWEI> display air-scan-profile name test
------------------------------------------------------------
Scan switch       : enable
Scan period(ms)   : 80
Scan interval(ms) : 3000
Scan channel-set  : dca-channel
Scan enhancement  : enable
------------------------------------------------------------
```

Table 11-133 Description of the **display air-scan-profile name** command output

Item	Description
Scan switch	Whether air scanning is enabled. To configure the parameter, run the **scan-disable** command.
Scan period(ms)	Air scan period. To set the air scan period, run the **scan-period** command.
Scan interval(ms)	Air scan interval. To set the air scan interval, run the **scan-interval** command.
Scan channel-set	Air scan channel set. To set the air scan channel set, run the **scan-channel-set** command.
Scan enhancement	Whether the scanning enhancement function is enabled. To configure the scanning enhancement function, run the **scan-enhancement** command.

11.4.50 display anti-interference config

Function

The **display anti-interference config** command displays the configuration of the anti-interference algorithm.

Format

display anti-interference config

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display anti-interference config** command displays the configuration of the anti-interference algorithm.

Example

Display the configuration of the anti-interference algorithm.

```
<HUAWEI> display anti-interference config
------------------------------------------
Anti-interference switch       : enable
Per-packet-TPC switch          : enable
AGC check switch               : enable
Dynamic CCA upper threshold    : -70
Dynamic CCA lower threshold    : -82
Edge STA SNR threshold         : 22
Edge STA RSSI threshold        : -70
------------------------------------------
```

Table 11-134 Description of the **display anti-interference config** command output

Item	Description
Anti-interference switch	Whether the anti-interference algorithm is enabled. To configure this parameter, run the **anti-interference disable** command.
Per-packet-TPC switch	Whether the packet-based power adjustment function is enabled. To configure this parameter, run the **anti-interference per-packet-tpc disable** command.

Item	Description
AGC check switch	Whether the AGC algorithm before packet transmission is enabled. To configure this parameter, run the **anti-interference agc-check disable** command.
Dynamic CCA upper threshold	Upper dynamic CCA threshold.
Dynamic CCA lower threshold	Lower dynamic CCA threshold.
Edge STA SNR threshold	Threshold for determining an edge STA based on the SNR.
Edge STA RSSI threshold	Threshold for determining an edge STA based on the RSSI.

11.4.51 display flexible-radio status

Function

The **display flexible-radio status** command displays the status and switching result of the redundant radio.

Format

display flexible-radio status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display flexible-radio status** command to check the status and switching result of the redundant radio.

Example

Display the status and switching result of the redundant radio.

```
<HUAWEI> display flexible-radio status
Redundancy Results:
R: The current radio is a redundant radio that has not been switched
```



```
S(5G): The redundant radio is switched to the 5 GHz mode
S(monitor): The redundant radio is switched to the monitor mode
S(off): This redundant radio is disabled
-: This radio is not a redundant radio
Recognize time: 2019-06-11/16:59:52 DST
------------------------------------------------------------
AP ID  Name           RfID  Band ST  Redundancy Result
------------------------------------------------------------
2      00e0-fc12-3455  0     2.4G on  R
3      00e0-fc12-3456  0     2.4G on  S(5G)
------------------------------------------------------------
Total:4
```

Table 11-135 Description of the **display flexible-radio status** command output

Item	Description
Recognize time	Time when the redundant radio is identified. **DST** indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
AP ID	AP ID.
Name	AP name.
RfID	Radio ID.
Band	Frequency band of the radio.
ST	Radio status.
Redundancy Result	Switching result of the redundant radio. ● R: The current radio is a redundant radio that has not been switched. ● S(5G): The redundant radio is switched to the 5 GHz mode. ● S(monitor): The redundant radio is switched to the monitor mode. ● S(off): This redundant radio is disabled. ● -: This radio is not a redundant radio.

11.4.52 display flexible-radio switch-record

Function

The **display flexible-radio switch-record** command displays the switching record of the redundant radio.

Format

display flexible-radio switch-record [**detail**]

Parameters

Parameter	Description	Value
detail	Displays the detailed switching record of the redundant radio.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display flexible-radio switch-record** command to check the switching record of the redundant radio.

Example

Display the switching record of the redundant radio.

```
<HUAWEI> display flexible-radio switch-record
-------------------------------------------------------------
Time                  ApID  Name          RfID  Switch
-------------------------------------------------------------
2019-06-10/20:45:58 DST   5     00e0-fc12-3456  0     monitor
-------------------------------------------------------------
Total : 1
```

Display the detailed switching record of the redundant radio.

```
<HUAWEI> display flexible-radio switch-record detail
-------------------------------------------------------------------------------------------------------------------------------
---------
Time                  ApID  Name          RfID  Switch   ReferenceRadio(ApID/ApName/PL)
-------------------------------------------------------------------------------------------------------------------------------
---------
2019-06-10/20:45:58 DST   5     00e0-fc12-3456  0     monitor  (0   /00e0-fc12-c220/52  ),(6   /00e0-fc12-
f7c0/40  ),(2   /00e0-fc7a-f9e0/52  )
-------------------------------------------------------------------------------------------------------------------------------
---------
Total : 1
```


Table 11-136 Description of the **display flexible-radio switch-record detail** command output

Item	Description
Time	Time when the redundant radio is switched. **DST** indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
ApID	AP ID.
Name	AP name.
RfID	Radio ID.
Switch	Switching result of the redundant radio. • 5G: The redundant radio is switched to the 5 GHz mode. • 2.4G: The redundant radio is switched back to the 2.4 GHz mode. • monitor: The redundant radio is switched to the monitor mode. • normal: The redundant radio is switched back to the normal mode. • off: This redundant radio is disabled. • on: This redundant radio is enabled.
ReferenceRadio(ApID/ApName/PL)	Top 3 neighbors of the redundant radio (AP ID/AP name/path loss).

11.4.53 display interference-visualization configuration

Function

The **display interference-visualization configuration** command displays information about AP radios on which interference visualization is enabled.

NOTE

Interference visualization is not available for the following models:

- AirEngine x761
- AirEngine x762

Format

display interference-visualization configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about AP radios on which interference visualization is enabled.

```
<HUAWEI> display interference-visualization configuration
-------------------------------------------------------------------------------
ID AP name Radio ID
-------------------------------------------------------------------------------
0  ap0     0
0  ap0     1
-------------------------------------------------------------------------------
Total: 2
```

Table 11-137 Description of the **display interference-visualization configuration** command output

Item	Description
ID	AP ID.
AP name	AP name.
Radio ID	Radio ID.

11.4.54 display references air-scan-profile

Function

The **display references air-scan-profile** command displays reference information about an air scan profile.

Format

display references air-scan-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified air scan profile.	The air scan profile name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references air-scan-profile** command to view reference information about an air scan profile.

Example

Display reference information about the air scan profile **test**.

```
<HUAWEI> display references air-scan-profile name test
------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------
radio-2g-profile            default
------------------------------------------------------------
Total: 1
```

Table 11-138 Description of the **display references air-scan-profile** command output

Item	Description
Reference type	Type of the profile that references the air scan profile.
Reference name	Name of the profile that references the air scan profile.

11.4.55 display references rrm-profile

Function

The **display references rrm-profile** command displays reference information about an RRM profile.

Format

display references rrm-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified RRM profile.	The RRM profile name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references rrm-profile** command to view reference information about an RRM profile.

Example

Display reference information about the RRM profile **default**

```
<HUAWEI> display references rrm-profile name default
------------------------------------------------------------
Reference type          Reference name
------------------------------------------------------------
radio-2g-profile        radio0
radio-5g-profile        radio1
------------------------------------------------------------
Total: 2
```

Table 11-139 Description of the **display references rrm-profile** command output

Item	Description
Reference type	Type of the profile that references the RRM profile.
Reference name	Name of the profile that references the RRM profile.

11.4.56 display references scene

Function

The **display references scene** command displays reference information about a scenario profile.

Format

display references scene name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified scenario profile.	The value is of the enumerated type. • multi-partition-cross-room: indicates an indoor multi-partition cross-room deployment scenario (capacity first). • multi-partition-cross-room-cov: indicates an indoor multi-partition cross-room deployment scenario (coverage first). • automated-guided-vehicle: indicates an AGV scenario. • high-density-stadium: indicates a high-density stadium scenario. • indoor-high-density: indicates an indoor high-density coverage scenario. • indoor-low-density: indicates an indoor low-density coverage scenario. • indoor-multi-partition: indicates an indoor multi-partition coverage scenario.

Parameter	Description	Value
		• indoor-normal-density: indicates an indoor common coverage scenario. • industrial-manufacturing: indicates an industrial manufacturing scenario. • outdoor-continuous: indicates an outdoor continuous coverage scenario. • virtual-reality: indicates a VR scenario.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view reference information about a scenario profile.

Example

Display reference information about the scenario profile **multi-partition-cross-room**.

```
<HUAWEI> display references scene name multi-partition-cross-room
------------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------------
AP group                    11
AP ID                       0
------------------------------------------------------------------------------
Total: 2
```


Table 11-140 Description of the **display references scene** command output

Item	Description
Reference type	Type of the entity that references a scenario profile. The type can be AP group or AP.
Reference name	Name of the entity that references a scenario profile. The name can be an AP group name or AP ID.

11.4.57 display rrm-profile

Function

The **display rrm-profile** command displays information about RRM profiles.

Format

display rrm-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all RRM profiles.	-
name *profile-name*	Displays information about a specified RRM profile.	The RRM profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rrm-profile** command to view information about RRM profiles.

Example

Display information about all RRM profiles.

```
<HUAWEI> display rrm-profile all
-------------------------------------------------------------
```



```
Profile name  Reference
--------------------------------------------------------------
default       2
--------------------------------------------------------------
Total:1
```

Table 11-141 Description of the **display rrm-profile all** command output

Item	Description
Profile name	Name of an RRM profile.
Reference	Number of times an RRM profile is referenced.

Display information about the RRM profile **default**.

```
<HUAWEI> display rrm-profile name default
------------------------------------------------------------------------
Retransmission rate threshold for trigger channel/power select(%)  : 55
Noise-floor threshold for trigger channel/power select(dBm)  : -75
Calibrate tpc threshold(dBm):                                 : -60
Maximum 2.4G calibration TX power(dBm)                        : 127
Maximum 5G calibration TX power(dBm)                          : 127
Maximum 6G calibration TX power(dBm)                          : 127
Minimum 2.4G calibration TX power(dBm)                        : 9
Minimum 5G calibration TX power(dBm)                          : 12
Minimum 6G calibration TX power(dBm)                          : 12
Calibrate retransmission rate check interval(min)             : 1
Calibrate retransmission rate check traffic threshold(kbps)  : 1250
Calibrate grouping interference threshold(dBm)                : -127
Airtime fairness schedule                                   : disable
Dynamic adjust EDCA parameter                                 : disable
Dynamic EDCA be-service threshold                             : 6
UAC check client's SNR                                      : disable
UAC client's SNR threshold(dB)                                : 20
UAC check client number                                     : disable
UAC client number access threshold                            : 64
UAC client number roam threshold                              : 64
Action upon reaching the UAC threshold                        : SSID broadcast
Band steer deny threshold                                   : 0
Band steer SNR threshold(dB)                                  : 20
Band balance start threshold                                : 100
Band balance gap threshold(%)                                 : 20
Client's band expire based on continuous probe counts         : 35
Station load balance                                        : disable
Station load balance mode                                     : sta-number
Station load balance RSSI threshold(dBm)                      : -70
Station load balance RSSI-diff-gap threshold(dBm)             : 20
Station load balance sta-number start threshold               : 10
Station load balance sta-number gap threshold(percentage)     : 20
Station load balance sta-number gap threshold(number)         : -
Station load balance deauth fail times                        : 2
Station load balance BTM fail times                         : 5
Station load balance steer-restrict restrict time(s)          : 5
Station load balance steer-restrict probe threshold           : 5
Station load balance steer-restrict auth  threshold           : 0
Station load balance probe-report interval(s)                 : 30
BSS color switch                                            : enable
Spatial reuse switch                                         : enable
Smart-roam                                                  : enable
Smart-roam AI mode                                            : disable
Smart-roam quick kickoff                                      : enable
Smart-roam check SNR                                          : enable
Smart-roam quick kickoff check SNR                            : enable
```



```
Smart-roam check rate                                : disable
Smart-roam quick kickoff check rate                  : disable
Smart-roam standing SNR threshold(dB)                : 20
Smart-roam SNR quick-kickoff-threshold(dB)           : 15
Smart-roam rate threshold(%)                         : 20
Smart-roam rate quick-kickoff-threshold(%)           : 20
Smart-roam high level SNR margin(dB)                 : 15
Smart-roam low level SNR margin(dB)                  : 6
Smart-roam SNR check interval(s)                     : 3
Smart-roam unable roam client expire time(min)       : 120
Smart-roam quick-kickoff SNR check interval(ms)      : 500
Smart-roam quick-kickoff SNR P-N observe time        : 6
Smart-roam quick-kickoff SNR P-N qualify time        : 4
Smart-roam advanced scan                             : enable
Smart-roam quick-kickoff back off time               : 60
AMC policy                                           : auto-balance
High density AMC optimize                            : disable
Antenna-mode                                         : omnidirection
SFN roam check high threshold(dBm)                   : -55
SFN roam check low threshold(dBm)                    : -60
SFN roam check interval(ms)                          : 700
SFN roam report interval(ms)                         : 400
SFN roam check rssi-accumulate threshold(dB)         : 8
SFN roam check sta-holding times                     : 3
SFN roam check gap-rssi(dB)                          : 6
SFN roam check better-times                          : 2
DFS smart select                                     : enable
DFS recover delay time(min)                          : 0
Multimedia air optimize
  Switch                                             : disable
  Voice threshold                                    : 30
  Video threshold                                    : 100
  Voice downlink-slice-ratio                         : medium
  Video downlink-slice-ratio                         : medium
  Voice downlink-delay-guarantee                     : medium
  Video downlink-delay-guarantee                     : medium
  Best effort downlink-delay-guarantee               : medium
  Background downlink-delay-guarantee                : medium
  Congestion-control tcp-window-tuning switch        : enable
  Uplink-delay-guarantee                             : enable
Rate limit dynamic interval                          : 5
Rate limit dynamic threshold                         : 80
CO-SR                                                : enable
Wlan-slice high-reliability
  Switch                                             : disable
  rtt                                                : 20
  time-ratio                                         : 80
  FRER-enhance                                       : disable
------------------------------------------------------------------------------
```

Table 11-142 Description of the **display rrm-profile name** command output

Item	Description
Retransmission rate threshold for trigger channel/power select(%)	Retransmission rate threshold for triggering channel or power adjustment. To configure this parameter, run the **calibrate retransmission-rate-threshold** command.

Item	Description
Noise-floor threshold for trigger channel/power select(dBm)	Noise-floor threshold for triggering channel or power adjustment. To configure this parameter, run the **calibrate noise-floor-threshold** command.
Calibrate tpc threshold(dBm)	Transmit Power Control (TPC) coverage threshold. To configure this parameter, run the **calibrate tpc threshold** command.
Maximum 2.4G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 2.4 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power** command.
Maximum 5G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 5 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power radio-5g** command.
Maximum 6G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 6 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power radio-6g** command.
Minimum 2.4G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 2.4 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power** command.
Minimum 5G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 5 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power radio-5g** command.
Minimum 6G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 6 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power radio-6g** command.

Item	Description
Calibrate retransmission rate check interval(min)	Interval for checking the retransmission rate. To configure this parameter, run the **calibrate retransmission-rate-check** command.
Calibrate retransmission rate check traffic threshold(kbps)	Traffic threshold for checking the retransmission rate. To configure this parameter, run the **calibrate retransmission-rate-check** command.
Calibrate grouping interference threshold(dBm)	RSSI interference threshold of a calibration group. To configure this parameter, run the **calibrate grouping interference-threshold** command.
Airtime fairness schedule	Whether airtime fair scheduling is enabled. To configure this parameter, run the **airtime-fair-schedule enable** command.
Dynamic adjust EDCA parameter	Whether dynamic EDCA parameter adjustment is enabled. To configure this parameter, run the **dynamic-edca enable** command.
Dynamic EDCA be-service threshold	Threshold for the dynamic EDCA Best-Effort service. To configure this parameter, run the **dynamic-edca threshold** command.
UAC check client's SNR	Whether user CAC based on the STA's SNR is enabled. To configure this parameter, run the **uac enable** command.
UAC client's SNR threshold(dB)	User CAC SNR threshold. To configure this parameter, run the **uac client-snr threshold** command.
UAC check client number	Whether user CAC based on the number of users is enabled. To configure this parameter, run the **uac enable** command.

Item	Description
UAC client number access threshold	User CAC access threshold based on the number of users. To configure this parameter, run the **uac client-number threshold** command.
UAC client number roam threshold	User CAC roaming threshold based on the number of users. To configure this parameter, run the **uac client-number threshold** command.
Action upon reaching the UAC threshold	Action to take when the number of access users reaches the user CAC threshold. ● SSID hide: hiding the SSID ● SSID broadcast: broadcasting the SSID ● priority-based STA replacement: allowing access of VIP users instead of non-VIP users based on priorities To configure this parameter, run the **uac reach-access-threshold** command.
Band steer deny threshold	Maximum number of times an AP rejects association requests of a STA for band steering. To configure this parameter, run the **band-steer deny-threshold** command.
Band steer SNR threshold(dB)	Start SNR threshold for triggering 5G-prior access. To configure this parameter, run the **band-steer snr-threshold** command.
Band balance start threshold	Start threshold for load balancing between radios. To configure this parameter, run the **band-steer balance start-threshold** command.
Band balance gap threshold(%)	Load difference threshold for load balancing between radios. To configure this parameter, run the **band-steer balance gap-threshold** command.

Item	Description
Client's band expire based on continuous probe counts	Aging condition of terminal band information, that is, the number of times that an AP has continuously received Probe frames of a terminal from the same frequency band. To configure this parameter, run the **band-steer client-band-expire** command.
Station load balance	Whether the load balancing function is enabled. To configure this parameter, run the **sta-load-balance dynamic disable** command.
Station load balance mode	Dynamic load balancing mode. sta-number: dynamic load balancing based on the number of STAs.
Station load balance RSSI threshold(dBm)	RSSI threshold of members in a dynamic load balancing group. To configure this parameter, run the **sta-load-balance dynamic rssi-threshold** command.
Station load balance RSSI-diff-gap threshold(dBm)	RSSI difference threshold for members in a dynamic load balancing group. To configure this parameter, run the **sta-load-balance dynamic rssi-diff-gap** command.
Station load balance sta-number start threshold	Start threshold for dynamic load balancing based on the number of users. To configure this parameter, run the **sta-load-balance dynamic sta-number start-threshold** command.
Station load balance sta-number gap threshold(percentage)	Load difference threshold for dynamic load balancing based on the percentage of users. To configure this parameter, run the **sta-load-balance dynamic sta-number gap-threshold** command.

Item	Description
Station load balance sta-number gap threshold(number)	Load difference threshold for dynamic load balancing based on the number of users. To configure this parameter, run the **sta-load-balance dynamic sta-number gap-threshold** command.
Station load balance deauth fail times	Maximum number of attempts to steer STAs in deauthentication mode. To configure this parameter, run the **sta-load-balance dynamic deauth-fail-times** command.
Station load balance BTM fail times	Maximum number of attempts to steer STAs in BTM mode. To configure this parameter, run the **sta-load-balance dynamic btm-fail-times** command.
Station load balance steer-restrict restrict time(s)	Duration within which non-target APs suppress association of STAs during STA steering. To configure this parameter, run the **sta-load-balance dynamic steer-restrict restrict-time** command.
Station load balance steer-restrict probe threshold	Maximum number of times non-target APs perform probe suppression for STAs during STA steering. To configure this parameter, run the **sta-load-balance dynamic steer-restrict probe-threshold** command.
Station load balance steer-restrict auth threshold	Maximum number of times non-target APs suppress authentication of STAs during STA steering. To configure this parameter, run the **sta-load-balance dynamic steer-restrict auth-threshold** command.
Station load balance probe-report interval(s)	Interval for reporting Probe frames. To configure this parameter, run the **sta-load-balance dynamic probe-report interval** command.
BSS color switch	Whether the BSS coloring function is enabled. To configure this parameter, run the **bss-color disable** command.

Item	Description
Spatial reuse switch	Whether the spatial reuse (SR) function is enabled. To configure this parameter, run the **spatial-reuse disable** command.
Smart-roam	Whether smart roaming is enabled. To configure this parameter, run the **smart-roam { enable | disable }** command.
Smart-roam AI mode	Whether the AI roaming function is enabled. To configure this parameter, run the **smart-roam ai-mode** command.
Smart-roam quick kickoff	Whether the function of quickly disconnecting STAs is enabled. To configure this parameter, run the **smart-roam quick-kickoff-threshold disable** command.
Smart-roam check SNR	Whether the trigger mode of smart roaming is specified as **check SNR**. To configure this parameter, run the **smart-roam roam-threshold { check-snr | check-rate }** command.
Smart-roam quick kickoff check SNR	Whether the function of quickly disconnecting STAs is triggered by checking the SNR of STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command.
Smart-roam check rate	Whether the trigger mode of smart roaming is specified as **check rate**. To configure this parameter, run the **smart-roam roam-threshold { check-snr | check-rate }** command.
Smart-roam quick kickoff check rate	Whether the function of quickly disconnecting STAs is triggered by checking the rate of STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command.

Item	Description
Smart-roam standing SNR threshold(dB)	SNR threshold for smart roaming. To configure this parameter, run the **smart-roam roam-threshold { snr | rate }** command.
Smart-roam SNR quick-kickoff-threshold(dB)	SNR threshold for quickly disconnecting STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold** command.
Smart-roam rate threshold(%)	Rate threshold for smart roaming. To configure this parameter, run the **smart-roam roam-threshold { snr | rate }** command.
Smart-roam rate quick-kickoff-threshold(%)	Rate threshold for quickly disconnecting STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold** command.
Smart-roam high level SNR margin(dB)	Higher SNR difference threshold that triggers STA roaming. To configure this parameter, run the **smart-roam snr-margin** command.
Smart-roam low level SNR margin(dB)	Lower SNR difference threshold that triggers STA roaming. To configure this parameter, run the **smart-roam snr-margin** command.
Smart-roam SNR check interval(s)	Interval for checking the SNR of STAs.
Smart-roam unable roam client expire time(min)	Aging time of "unable to roam" record. To configure this parameter, run the **smart-roam unable-roam-client expire-time** command.
Smart-roam quick-kickoff SNR check interval(ms)	Interval for checking the SNR to determine whether to quickly disconnect STAs. To configure this parameter, run the **smart-roam quick-kickoff-snr check-interval** command.

Item	Description
Smart-roam quick-kickoff SNR P-N observe time	Number of PN observation times to determine whether to quickly disconnect STAs. To configure this parameter, run the **smart-roam quick-kickoff-snr p-n criteria** command.
Smart-roam quick-kickoff SNR P-N qualify time	Number of PN observation times to determine whether to quickly disconnect STAs. To configure this parameter, run the **smart-roam quick-kickoff-snr p-n criteria** command.
Smart-roam advanced scan	Whether coordinated scanning function of smart roaming is enabled. To configure this parameter, run the **smart-roam advanced-scan disable** command.
Smart-roam quick-kickoff back off time	Backoff time for quickly disconnecting STAs. To configure this parameter, run the **smart-roam quick-kickoff back-off-time** command.
AMC policy	Adaptive modulation and coding (AMC) algorithm. To configure this parameter, run the **amc-policy** command.
High density AMC optimize	Whether the AMC optimization function in high-density scenarios is enabled. To configure this parameter, run the **high-density amc-optimize enable** command.
Antenna-mode	Antenna mode. To configure this parameter, run the **antenna-mode** command.
SFN roam check high threshold(dBm)	Upper RSSI threshold for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check high-threshold** command.

Item	Description
SFN roam check low threshold(dBm)	Lower RSSI threshold for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check low-threshold** command.
SFN roam check interval(ms)	Decision period for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check check-interval** command.
SFN roam report interval(ms)	Interval for RUs to report the STA RSSI. To configure this parameter, run the **sfn-roam report-interval** command.
SFN roam check rssi-accumulate threshold(dB)	Cumulative RSSI change threshold for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check rssi-accumulate** command.
SFN roam check sta-holding times	Number of STA holding times for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check sta-holding times** command.
SFN roam check gap-rssi(dB)	RSSI gap for agile distributed SFN roaming RUs. To configure this parameter, run the **sfn-roam roam-check gap-rssi** command.
SFN roam check better-times	Number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU. To configure this parameter, run the **sfn-roam roam-check better-times** command.

Item	Description
DFS smart select	Whether DFS smart selection is enabled. ● enable: DFS smart selection is enabled. ● disable: DFS smart selection is disabled. To configure this parameter, run the **dfs smart-selection disable** command.
DFS recover delay time(min)	Delay in switching back the DFS channel. To configure this parameter, run the **dfs recover-delay** command.
Switch	Whether the intelligent multimedia scheduling algorithm is enabled. ● disable: The intelligent multimedia scheduling algorithm is disabled. ● enable: The intelligent multimedia scheduling algorithm is enabled. To configure this parameter, run the **multimedia-air-optimize disable** command.
Voice threshold	Voice packet threshold. To configure this parameter, run the **multimedia-air-optimize threshold** command.
Video threshold	Video packet threshold. To configure this parameter, run the **multimedia-air-optimize threshold** command.
Voice downlink-slice-ratio	Slicing ratio for voice packets. To configure this parameter, run the **multimedia-air-optimize downlink-slice-ratio** command.
Video downlink-slice-ratio	Slicing ratio for video packets. To configure this parameter, run the **multimedia-air-optimize downlink-slice-ratio** command.
Voice downlink-delay-guarantee	Guaranteed delay for voice packets. To configure this parameter, run the **multimedia-air-optimize downlink-delay-guarantee** command.

Item	Description
Video downlink-delay-guarantee	Guaranteed delay for video packets. To configure this parameter, run the **multimedia-air-optimize downlink-delay-guarantee** command.
Best effort downlink-delay-guarantee	Guaranteed delay for BE flows. To configure this parameter, run the **multimedia-air-optimize downlink-delay-guarantee** command.
Background downlink-delay-guarantee	Guaranteed delay for BK flows. To configure this parameter, run the **multimedia-air-optimize downlink-delay-guarantee** command.
Congestion-control tcp-window-tuning switch	Whether the TCP window adjustment function for voice and video services is enabled. • disable: The TCP window adjustment function for voice and video services is disabled. • enable: The TCP window adjustment function for voice and video services is enabled. To configure this parameter, run the **multimedia-air-optimize congestion-control tcp-window-tuning disable** command.
Uplink-delay-guarantee	Whether the delay guarantee function for uplink services is enabled. • disable: The function is disabled. • enable: The function is enabled. To configure this parameter, run the **multimedia-air-optimize uplink-delay-guarantee disable** command.
Rate limit dynamic interval	Detection interval for dynamic rate limiting. To configure this parameter, run the **rate-limit dynamic interval** command.
Rate limit dynamic threshold	Detection threshold for dynamic rate limiting. To configure this parameter, run the **rate-limit dynamic interval** command.

Item	Description
CO-SR	Whether the CoSR function is enabled. • disable: The function is disabled. • enable: The function is enabled. To configure this parameter, run the **co-sr disable** command.
Switch	Whether the WLAN high-reliability slicing function is enabled. To configure this parameter, run the **wlan-slice high-reliability enable** command.
rtt	Expected RTT of WLAN high-reliability slicing. To configure this parameter, run the **wlan-slice high-reliability rtt** command.
time-ratio	Time proportion of WLAN high-reliability slicing. To configure this parameter, run the **wlan-slice high-reliability time-ratio** command.
FRER-enhance	Whether the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios is enabled. To configure this parameter, run the **wlan-slice high-reliability frer-enhance** command.

11.4.58 display sta-load-balance static-group

Function

The **display sta-load-balance static-group** command displays information about static load balancing groups.

Format

display sta-load-balance static-group { **all** | **name** *group-name* }

Parameters

Parameter	Description	Value
all	Displays information about all static load balancing groups.	-
name *group-name*	Displays information about a specified static load balancing group.	The static load balancing group must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display sta-load-balance static-group** command to view information about a specified static load balancing group or all static load balancing groups.

Example

Display information about all static load balancing groups.

```
<HUAWEI> display sta-load-balance static-group all
-------------------------------------------------------------
Index  Group name
-------------------------------------------------------------
0      cc
1      coco
-------------------------------------------------------------
Total: 2
```

Table 11-143 Description of the **display sta-load-balance static-group all** command output

Item	Description
Index	Index.
Group name	Name of a static load balancing group.

Display information about the static load balancing group **cc**.

```
<HUAWEI> display sta-load-balance static-group name cc
-------------------------------------------------------------------
Group name                    : cc
Load-balance mode             : sta-number
Sta-number start threshold    : 40
```



```
Sta-number gap threshold(percentage)   : 20
Sta-number gap threshold(number)       : -
RSSI threshold(dBm)                    : -70
RSSI diff gap(dBm)                     : 5
Deauth fail times                      : 2
Btm fail times                         : 5
Steer-restrict restrict time(s)        : 5
Steer-restrict probe threshold         : 5
Steer-restrict auth threshold          : 2
------------------------------------------------------------------------
```

Table 11-144 Description of the **display sta-load-balance static-group name** command output

Item	Description
Group name	Name of a static load balancing group.
Load-balance mode	Static load balancing mode. • sta-number: static load balancing based on the number of users
Sta-number start threshold	Start threshold for load balancing based on the number of users in the static load balancing group. To configure this parameter, run the **sta-number start-threshold** command.
Sta-number gap threshold(percentage)	Load difference threshold for static load balancing based on the percentage of users. To configure this parameter, run the **sta-number gap-threshold** command.
Sta-number gap threshold(number)	Load difference threshold for static load balancing based on the number of users. To configure this parameter, run the **sta-number gap-threshold** command.
RSSI threshold(dBm)	RSSI threshold of members in the static load balancing group. To configure this parameter, run the **rssi-threshold** command.
RSSI diff gap(dBm)	RSSI difference threshold of members in the static load balancing group. To configure this parameter, run the **rssi-diff-gap** command.
Deauth fail times	Maximum number of attempts to steer STAs in deauthentication mode. To configure this parameter, run the **deauth-fail-times** command.

Item	Description
Btm fail times	Maximum number of attempts to steer STAs in BTM mode. To configure this parameter, run the **btm-fail-times** command.
Steer-restrict restrict time(s)	Duration within which non-target APs suppress association of STAs during STA steering. To configure this parameter, run the **steer-restrict restrict-time** command.
Steer-restrict probe threshold	Maximum number of times non-target APs suppress probing of STAs during STA steering. To configure this parameter, run the **steer-restrict probe-threshold** command.
Steer-restrict auth threshold	Maximum number of times non-target APs suppress authentication of STAs during STA steering. To configure this parameter, run the **steer-restrict auth-threshold** command.

11.4.59 display sta-load-balance fairness

Function

The **display sta-load-balance fairness** command displays the load balancing fairness.

Format

display sta-load-balance fairness

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

STAs may access 2.4 GHz or 5 GHz radios on a WLAN. Even STA access indicates high fairness.

Example

Display the load balancing fairness.

```
<HUAWEI> display sta-load-balance fairness
2.4G sta-load-balance fairness : -
5G sta-load-balance fairness   : 0.85
```

Table 11-145 Description of the **display sta-load-balance fairness** command output

Item	Description
2.4G sta-load-balance fairness	Load balancing fairness of 2.4 GHz radios. A high value indicates high fairness. The value ranges from 0 to 1. When the value is 0, **-** is displayed.
5G sta-load-balance fairness	Load balancing fairness of 5 GHz radios. A high value indicates high fairness. The value ranges from 0 to 1. When the value is 0, **-** is displayed.

11.4.60 display station neighbor

Function

The **display station neighbor** command displays the neighbor list of a specified STA.

Format

display station neighbor sta-mac *mac-address*

Parameters

Parameter	Description	Value
sta-mac *mac-address*	Specifies the MAC address of a STA.	The MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the neighbor list of the STA with a specified MAC address.

Example

Display the neighbor list of the STA with a specified MAC address.

```
<HUAWEI> display station neighbor sta-mac 00e0-fc00-0001
UL info: Uplink measurement neighbor info
DL info: Downlink measurement neighbor info
-------------------------------------------------------------------------------------------------------------------------
--
Device MAC        Device ID   Device Name       Radio ID  Channel  UL info[RSSI/DATE]       DL info[RCPI/
RSSI/RSNI/DATE]
-------------------------------------------------------------------------------------------------------------------------
--
00e0-fc76-e360    0           00e0-fc76-e360    1         165      -44/2023-03-01/09:49:39  130/-45/-/
2023-03-01/09:49:39
-------------------------------------------------------------------------------------------------------------------------
--
Total neighbors: 1, total records: 1
```

System Response

Table 11-146 Description of the **display station neighbor** command output

Item	Description
Device MAC	MAC address of a neighboring device.
Device ID	ID of a neighboring device.
Device Name	Name of a neighboring device.
Radio ID	Radio ID of a neighboring device.
Channel	Channel of a neighboring device.
UL info[RSSI/DATE]	RSSI: signal strength of the neighboring device measured in the uplink direction, in dBm. DATE: timestamp. **NOTE** If a hyphen (-) is displayed, the STA does not support or perform uplink scanning.

Item	Description
DL info[RCPI/RSSI/RSNI/DATE]	RCPI: received channel power indicator (RCPI) of the neighbor device measured in the downlink direction, in dBm. RSSI: RSSI converted from the RCPI of the neighboring device measured in the downlink direction, in dBm. RSNI: received signal-to-noise indicator (RSNI), in dB DATE: timestamp. **NOTE** If a hyphen (-) is displayed, the STA does not support or perform downlink scanning, or an invalid value is returned.

11.4.61 display station neighbor all

Function

The **display station neighbor all** command displays STA neighbor information.

Format

display station neighbor all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view STA neighbor information.

Example

Display STA neighbor information.

```
<HUAWEI> display station neighbor all
UL neighbor number    : Number of neighbors detected through uplink measurement in 5 minutes
DL neighbor number    : Number of neighbors detected through downlink measurement in 5 minutes
Last update time      : Time when neighbors are detected through uplink or downlink measurement in 5
minutes
                        formatted: uplink/downlink
--------------------------------------------------------------------------------------------------------
```



```
STA MAC          UL neighbor number    DL neighbor number      Last update time
-------------------------------------------------------------------------------------------------------------
00e0-fca2-a1c5   2                     2                       2022-10-14/14:07:02/2022-10-14/14:04:06
-------------------------------------------------------------------------------------------------------------
Total:1
```

Table 11-147 Description of the **display station neighbor all** command output

Item	Description
STA MAC	MAC address of a STA.
UL neighbor number	Number of neighbors measured in the uplink direction in 5 minutes.
DL neighbor number	Number of neighbors measured in the downlink direction in 5 minutes.
Last update time	Time when a neighbor is detected in 5 minutes (uplink/downlink measurement).

11.4.62 display station steer-history

Function

The **display station steer-history** command displays historical information about STA steering.

Format

display station steer-history

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the load balancing, band steering, or smart roaming function is enabled, STAs are steered. You can run this command to check historical information about STA steering.

Example

Display historical information about steering of all STAs.


```
<HUAWEI> display station steer-history
S/T/A:Source/Target/Actual
Flag:P[AI Profiling STA] V[Voice/Video/Active STA]
BTM success times/BTM total times:2/4
Deauth success times/Deauth total times:0/0
-------------------------------------------------------------------------------------------------------------------------------
--------
Time              Sta           Device(S/T/A)   Radio(S/T/A)  Rssi(S/T/A)       Reason      Move-mode
BTM_CODE  Flag  Result
-------------------------------------------------------------------------------------------------------------------------------
--------
2019-01-11/15:56:49 00e0-fc12-3456  3/5/5          0/1/1       -27/-27/-25       BandSteer    BTM
-       -     Success
2019-01-11/15:48:49 00e0-fc12-3456  3/3/3          0/1/1       -28/-/-57         BandSteer    BTM
-       -     Success
2019-01-11/15:43:49 00e0-fc12-3456  3/5/3          0/1/0       -29/-26/-44       BandSteer    BTM
-       -     Not Move
2019-01-11/15:43:29 00e0-fc12-3456  3/5/3          0/1/0       -29/-26/-44       Sticky       BTM       -
-     Not Move
-------------------------------------------------------------------------------------------------------------------------------
--------
Total: 4
```

Table 11-148 Description of the **display station steer-history** command output

Item	Description
Time	Time when a STA is triggered to steer.
Sta	MAC address of a STA.
Device(S/T/A)	ID of the source device/ID of the target device/ID of the device to which a STA is actually steered.
Radio(S/T/A)	ID of the source radio/ID of the target radio/ID of the radio to which a STA is actually steered.
Rssi(S/T/A)	RSSI of the source radio/RSSI of the target radio/RSSI of the radio to which a STA is actually steered.
Reason	Reason why a STA is triggered to steer. ● Sticky: Smart roaming is enabled. ● Sticky(A): The device periodically detects whether the STA is a sticky STA to proactively trigger smart roaming. ● LoadBalance: Load balancing is enabled. ● BandSteer: Band steering is enabled. ● AI: AI roaming is enabled.
Move-mode	Steering mode of a STA. ● BTM ● Deauth

Item	Description
BTM_CODE	BTM steering status code. ● 0: Accept ● 1: Reject-Unspecified reject reason. ● 2: Reject-Insufficient Beacon or Probe Response frames received from all candidates. ● 3: Reject-Insufficient available capacity from all candidates. ● 4: Reject-BSS termination undesired. ● 5: Reject-BSS termination delay requested. ● 6: Reject-STA BSS Transition Candidate List provided. ● 7: Reject-No suitable BSS transition candidates. ● 8: Reject-Leaving ESS. ● -: A STA is steered in deauthentication mode or the device does not receive any BTM response.
Flag	● V: voice/video/active STA flag ● P: steering flag by STA profile ● -: other

Item	Description
Result	Steering result of a STA. • Success: The steering is successful. • Success(NT): The steering is successful but the STA is not steered to the expected target. • Time Out: The steering times out. • Not Move: The steering is complete, but the STA is still associated with the source AP. • Failed: The steering fails. (The steering result does not meet the expectation. For example, the STA is not steered to the 5 GHz radio in the band steering scenario, is steered to an AP with poor signal quality in the smart roaming scenario, or is steered to a high-load AP in the load balancing scenario.) • Protect: The AP detects that the STA is a voice, video, or active STA and protects the STA by not sending a steering message. • Error(1) or Error(2): An internal error occurs during the steering.

11.4.63 display station steer-info

Function

The **display station steer-info** command displays STA migration information based on the weak RSSI, non-optimal load, and migration inability.

Format

display station steer-info { **all** | **weak-rssi** | **non-best-load** | **unsteerable** }

Parameters

Parameter	Description	Value
all	Displays migration information about all STAs, including the weak RSSI, non-optimal load, and migration inability.	-

Parameter	Description	Value
weak-rssi	Displays STA information based on the weak RSSI.	-
non-best-load	Displays STA information based on the non-optimal load.	-
unsteerable	Displays STA information based on the migration inability.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view STA migration information based on the weak RSSI, non-optimal load, and migration inability.

Example

Display migration information about all STAs, including the weak RSSI, non-optimal load, and migration inability.

```
<HUAWEI> display station steer-info all
--------------------------------------------------------------------------
Sta-MAC             Weak RSSI       Non-best-load    Unsteerable
--------------------------------------------------------------------------
00e0-fc12-3456        Y               N                Y
--------------------------------------------------------------------------
Total STA          : 1
Weak-RSSI STA      : 1
Non-best-load STA  : 0
Unsteerable STA    : 1
```

Table 11-149 Description of the **display station steer-info** command output

Item	Description
Sta-MAC	MAC address of a STA.
Weak RSSI	Whether a STA has a weak RSSI.
Non-best-load	Whether a STA has the non-optimal load.
Unsteerable	Whether the STA cannot be migrated.

11.4.64 display station steer-statistics

Function

The **display station steer-statistics** command displays STA steering statistics.

Format

display station steer-statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the load balancing, band steering, or smart roaming function is enabled, STAs are steered. You can run this command to check STA steering statistics.

Example

Display steering statistics of all STAs.

```
<HUAWEI> display station steer-statistics
------------------------------------------------------------------------------------------------------------------------
------
Reason                    Total/Success       Deauth(Total/Success)   BTM(Total/Accept/REJ1/REJ2/REJ3/REJ4/
REJ5/REJ6/REJ7/REJ8/TimeOut)
------------------------------------------------------------------------------------------------------------------------
------
Sticky(Tradition)          58706/30430         0/0                  58706/30430/1083/0/0/9/0/241/7805/0/6446
Sticky(Profile)            58706/30430         0/0                  58706/30430/1083/0/0/9/0/241/7805/0/6446
Sticky(Profile Blind)      58706/30430         0/0                  58706/30430/1083/0/0/9/0/241/7805/0/6446
Load-balance(Tradition)     2450/1652          0/0                   2450/1652/4/0/0/0/0/20/335/0/20
Load-balance(Profile)       2450/1652          0/0                   2450/1652/4/0/0/0/0/20/335/0/20
Load-balance(Profile Blind) 2450/1652          0/0                   2450/1652/4/0/0/0/0/20/335/0/20
Band-steer(Tradition)       7596/2226          0/0                   7596/2226/39/0/0/29/0/131/968/0/335
Band-steer(Profile)         7596/2226          0/0                   7596/2226/39/0/0/29/0/131/968/0/335
Band-steer(Profile Blind)   7596/2226          0/0                   7596/2226/39/0/0/29/0/131/968/0/335
AI                        13256/10349          0/0                 13256/10349/0/0/0/0/0/0/0/0/58
Total                      82008/44657         0/0                  82008/44657/1126/0/0/38/0/392/9108/0/6859
------------------------------------------------------------------------------------------------------------------------
------
```


Table 11-150 Description of the **display station steer-statistics** command output

Item	Description
Reason	Reason why a STA is triggered to steer. • Sticky(Tradition): The STA is sticky (STA steering triggered by traditional smart roaming). • Sticky(Profile): The STA is sticky (STA steering based on STA profiles, not blind handover). • Sticky(Profile Blind): The STA is sticky (STA steering based on STA profiles, blind handover). • Load-balance(Tradition): Load balancing is implemented (STA steering triggered by traditional smart roaming). • Load-balance(Profile): Load balancing is implemented (STA steering based on STA profiles, not blind handover). • Load-balance(Profile Blind): Load balancing is implemented (STA steering based on STA profiles, blind handover). • Band-steer(Tradition): Band steering is implemented (STA steering triggered by traditional smart roaming). • Band-steer(Profile): Band steering is implemented (STA steering based on STA profiles, not blind handover). • Band-steer(Profile Blind): Band steering is implemented (STA steering based on STA profiles, blind handover). • AI: AI roaming steering based on coordinated scanning is implemented. • Total: total steering reason count.
Total/Success	Total number of triggered STA steering times/Number of successful STA steering times.

Item	Description
Deauth(Total/Success)	Total number of times STA steering is triggered in deauthentication mode/ Number of times STA steering is successfully triggered in deauthentication mode.
BTM(Total/Accept/REJ1/REJ2/REJ3/ REJ4/REJ5/REJ6/REJ7/REJ8/TimeOut)	Total number of times STA steering is triggered in BTM mode/Number of times STA steering is successfully triggered in BTM mode/Number of times STA steering is rejected in BTM mode/Number of times STA steering is timed out in BTM mode. The options are as follows: • REJ1: Reject-Unspecified reject reason. • REJ2: Reject-Insufficient Beacon or Probe Response frames received from all candidates. • REJ3: Reject-Insufficient available capacity from all candidates. • REJ4: Reject-BSS termination undesired. • REJ5: Reject-BSS termination delay requested. • REJ6: Reject-STA BSS Transition Candidate List provided. • REJ7: Reject-No suitable BSS transition candidates. • REJ8: Reject-Leaving ESS.

11.4.65 display station unsteerable

Function

The **display station unsteerable** command displays "unable to roam" records of STAs.

Format

display station unsteerable

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display station unsteerable** command to check "unable to roam" records of STAs.

Example

Display "unable to roam" records of STAs.

```
<HUAWEI> display station unsteerable
--------------------------------------------------------------------------------
STA MAC             Left aging time         Status
--------------------------------------------------------------------------------
00e0-fc12-3456      3h 20m                  online
00e0-fc45-7890      2h 30m                  offline
--------------------------------------------------------------------------------
Total: 2
```

Table 11-151 Description of the **display station unsteerable** command output

Item	Description
STA MAC	MAC address of the "unable to roam" STA.
Left aging time	Remaining aging period.
Status	Status of the STA. • online • offline

11.4.66 display sta-profiling

Function

The **display sta-profiling** command displays STA profile information on the device.

Format

display sta-profiling

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

STAs of different models use different Wi-Fi chips and WLAN module drivers, and therefore have different roaming steering behaviors. To improve roaming experience, WLAN devices need to use different roaming steering policies for STAs of different types (distinguished by STA profiles). During the steering roaming for a STA, the system matches STA information against the existing STA profiles based on the model and operating system, and selects a more suitable roaming steering policy, improving the roaming success rate. You can run the **display sta-profiling** command to check information about the learned STA profiles on the device.

Prerequisites

The STA profiling function has been enabled using the **undo sta-profiling disable** command.

Example

Display STA profile information on the device.

```
<HUAWEI> display sta-profiling
-------------------------------------------------------------------------------------------------
Vendor   Type                 Type ID      OS              OS ID      Priority   Version
-------------------------------------------------------------------------------------------------
...
Huawei   Mate 40               32455        Android 10      17765      1190       0
Huawei   Mate 40 Pro           32454        Android 10      17765      1188       0
Huawei   Mate 40 Pro Plus      32456        Android 10      17765      1192       0
Huawei   Mate RS               7348         Android 10      17765      149        0
...
-------------------------------------------------------------------------------------------------
 Total:313
```

Table 11-152 Description of the **display sta-profiling** command output

Item	Description
Vendor	Terminal brand.
Type	STA model.
Type ID	STA model ID.
OS	STA operating system.
OS ID	STA operating system ID.

Item	Description
Priority	Priority of the matching between a STA profile and the STA. A smaller value indicates a higher priority. If a STA matches multiple profiles based on the model and operating system, the profile with the highest priority is used.
Version	STA profile version. This version number increases with STA profile updates.

11.4.67 display wlan calibrate channel-set

Function

The **display wlan calibrate channel-set** command displays the effective calibration channels and bandwidth.

Format

display wlan calibrate channel-set ap-group { **name** *ap-group-name* | **all** }

Parameters

Parameter	Description	Value
ap-group name *ap-group-name*	Displays the effective calibration channels and bandwidth in a specified AP group.	The AP group must exist.
ap-group all	Displays the effective calibration channels and bandwidth in all AP groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the radio calibration function, you can run the **display wlan calibrate channel-set** command to check the effective calibration channels and bandwidth.

Example

Display the calibration channels and bandwidth that take effect globally.

```
<HUAWEI> display wlan calibrate channel-set ap-group all
AP group    : default
Country code: CN
--------------------------------------------------------------------------------
Radio band  Bandwidth  Channel Set
--------------------------------------------------------------------------------
2.4G        20MHz      1,6,11
5G          20MHz      149,153,157,161,165
6G          20MHz      -
--------------------------------------------------------------------------------

AP group    : mainland
Country code: CN
--------------------------------------------------------------------------------
Radio band  Bandwidth  Channel Set
--------------------------------------------------------------------------------
2.4G        20MHz      1,6,11
5G          20MHz      149,153,157,161,165
6G          20MHz      -
--------------------------------------------------------------------------------
```

Table 11-153 Description of the **display wlan calibrate channel-set** command output

Item	Description
AP group	Name of an AP group.
Country code	Country code.
Radio band	Radio type.
Bandwidth	Effective calibration bandwidth.
Channel Set	Effective calibration channel set.

11.4.68 display wlan calibrate global configuration

Function

The **display wlan calibrate global configuration** command displays the global configuration of radio calibration.

Format

display wlan calibrate global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan calibrate global configuration** command to check the global configuration of radio calibration.

Example

Display the global configuration of radio calibration.

```
<HUAWEI> display wlan calibrate global configuration
------------------------------------------------------------------------------
----------
Mode                                    : manual
Auto start time                         : -
Auto interval(min)                      : -
Schedule time                           : -
Schedule time-range                     : -
Calibration progress                    : 50%
Flexible radio mode                     : auto-switch
Policy                                  : -
2.4G sensitivity                        : low
5G sensitivity                          : high
6G sensitivity                          : medium
Virtual group size                      : 50
K-value                                 : 70
Reference data analysis                 : enable
Reference rogue ap interference         : enable
Environment deterioration blacklist threshold   : 16
------------------------------------------------------------------------------
----------
```

Table 11-154 Description of the **display wlan calibrate global configuration** command output

Item	Description
Mode	Radio calibration mode. To configure this parameter, run the **calibrate enable** { **auto** | **manual** | **schedule time** } command.
Auto start time	Start time of automatic radio calibration (only for the automatic radio calibration mode). To configure this parameter, run the **calibrate enable auto** [**interval** *interval-value* [**start-time** *start-time*]] command.

Item	Description
Auto interval(min)	Interval for automatic radio calibration (only for the automatic radio calibration mode). To configure this parameter, run the **calibrate enable auto** [**interval** *interval-value* [**start-time** *start-time*]] command.
Schedule time	Time of scheduled radio calibration (only for the scheduled radio calibration mode). To configure this parameter, run the **calibrate enable schedule time** *time-value* command.
Schedule time-range	Time range for scheduled radio calibration (only for the scheduled radio calibration mode). To configure this parameter, run the **calibrate enable schedule time** *time-value* [**time-range** *time-range-name*] command.
Calibration progress	Progress of manual or scheduled radio calibration.
Flexible radio mode	Redundant radio switchover mode. To configure this parameter, run the **calibrate flexible-radio** { **auto-switch** | **auto-off** } command.
Policy	Radio calibration policy. To configure this parameter, run the **calibrate policy** { **non-wifi** | **noise-floor** } command.
2.4G sensitivity 5G sensitivity 6G sensitivity	Radio calibration sensitivity. To configure this parameter, run the **calibrate sensitivity** [**2.4g** | **5g** | **6g**] { **high** | **medium** | **low** | **insensitivity** | **custom-percent** *custom-percent* } command.
Virtual group size	Parameter of the radio calibration algorithm. To configure this parameter, run the **calibrate virtual-group-size** *size-value* **k-value** *k-value* command.

Item	Description
K-value	Parameter of the radio calibration algorithm. To configure this parameter, run the **calibrate virtual-group-size** *size-value* **k-value** *k-value* command.
Reference data analysis	Whether to enable Big Data calibration. To configure this parameter, run the **calibrate reference data-analysis disable** command.
Reference rogue ap interference	Whether rogue interference calibration is enabled. To configure this parameter, run the **calibrate reference rogue-ap-interference disable** command.
Environment deterioration blacklist threshold	Blacklist threshold for the number of times the channel environment deteriorates. To configure this parameter, run the **calibrate environment-deterioration-blacklist threshold** command.

11.4.69 display wlan calibrate statistics

Function

The **display wlan calibrate statistics** command displays radio calibration statistics.

Format

display wlan calibrate statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays radio calibration statistics on the specified AP name. The AP name and radio ID together identify a radio.	The AP name must already exist.
ap-id *ap-id*	Displays radio calibration statistics on the specified AP ID. The AP ID and radio ID together identify a radio.	The AP ID must already exist.

Parameter	Description	Value
radio *radio-id*	Displays radio calibration statistics on the specified radio.	The radio ID must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan calibrate statistics** command to view radio calibration statistics, helping check whether the radio environment is stable.

Example

Display calibration statistics about radio 0 on AP0.

```
<HUAWEI> display wlan calibrate statistics ap-id 0 radio 0
------------------------------------------------------------------------
Signal environment deterioration :1
Power calibration                :1
Channel calibration              :0
------------------------------------------------------------------------
```

Table 11-155 Description of the **display wlan calibrate statistics** command output

Item	Description
Signal environment deterioration	Number of times the radio environment deteriorates.
Power calibration	Number of times the power of the radio is calibrated.
Channel calibration	Number of times the channel of the radio is calibrated.

11.4.70 display wlan scene

Function

The **display wlan scene** command displays information about a scenario profile.

Format

display wlan scene { **name** *scene-name* | **all** }

Parameters

Parameter	Description	Value
name *scene-name*	Specifies the name of a scenario profile.	The value is of the enumerated type. ● multi-partition-cross-room: indicates an indoor multi-partition cross-room deployment scenario (capacity first). ● multi-partition-cross-room-cov: indicates an indoor multi-partition cross-room deployment scenario (coverage first). ● automated-guided-vehicle: indicates an AGV scenario. ● high-density-stadium: indicates a high-density stadium scenario. ● indoor-high-density: indicates an indoor high-density coverage scenario. ● indoor-low-density: indicates an indoor low-density coverage scenario. ● indoor-multi-partition: indicates an indoor multi-partition coverage scenario. ● indoor-normal-density: indicates an indoor common coverage scenario. ● industrial-manufacturing: indicates an industrial manufacturing scenario. ● outdoor-continuous: indicates an outdoor continuous coverage scenario.

Parameter	Description	Value
		• virtual-reality: indicates a VR scenario.
all	Displays all scenario profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan scene** command to view detailed information about a scenario profile to learn about wireless service parameters and their settings involved in the scenario.

Example

Display all scenario profiles.

```
<HUAWEI> display wlan scene all
-------------------------------------------------------------------------------
Name                        Description
-------------------------------------------------------------------------------
automated-guided-vehicle      Applicable to smart warehousing scenarios.
high-density-stadium          Applicable to high-density stadiums.
indoor-high-density           Applicable to indoor high-density scenarios, such as cafes and high-density
office.
indoor-low-density            Applicable to indoor low-density scenarios, such as retail scenarios.
indoor-multi-partition        Applicable to indoor multi-partition scenarios, such as dormitories, hotel
rooms, and wards.
indoor-normal-density         Applicable to indoor normal-density scenarios, such as normal office.
industrial-manufacturing      Applicable to industrial manufacturing scenarios.
multi-partition-cross-room    Applicable to indoor scenarios (capacity first), where one AP covers multiple
rooms and APs are blocked from each other by walls.
multi-partition-cross-room-cov  Applicable to indoor scenarios (coverage first), where one AP covers
multiple rooms and APs are blocked from each other by walls.
outdoor-continuous            Applicable to outdoor continuous coverage scenarios, such as roadways and
parks.
virtual-reality               Applicable to VR scenarios.
-------------------------------------------------------------------------------
Total: 11
```

Display information about the scenario profile **multi-partition-cross-room**.

```
<HUAWEI> display wlan scene name multi-partition-cross-room
-------------------------------------------------------------------------------
Radio parameter:
  CCA threshold(dBm)                : -
  RX sensitivity(dBm)               : -
  Beacon interval(TUs)              : -
  Dynamic EDCA                      : enable
SSID parameter:
```



```
  Deny-broadcast-probe                : -
  Active dull client                  : -
  Association timeout(min)            : -
Station load balance:
  Sta-number start threshold          : -
  Sta-number gap threshold(number)    : -
Smart roam:
  Standing SNR threshold(dB)          : 15
  SNR quick-kickoff-threshold(dB)     : 10
Radio calibration:
  DCA 5G bandwidth                    : 80Mhz
  TPC threshold(dBm)                  : -35
  Grouping interference threshold(dBm)  : -70
  Maximum 2.4G calibration TX power(dBm)  : -
  Maximum 5G calibration TX power(dBm)  : -
  Minimum 2.4G calibration TX power(dBm)  : -
  Minimum 5G calibration TX power(dBm)  : -
------------------------------------------------------------------------------
```

Table 11-156 Description of the **display wlan scene** command output

Item	Description
WLAN service parameters	To view the description of a specific parameter, search for the parameter and view the description in the corresponding display command. If a hyphen (-) is displayed, this parameter is not configured in the scenario profile.

11.4.71 dynamic-edca enable

Function

The **dynamic-edca enable** command enables dynamic EDCA parameter adjustment.

The **undo dynamic-edca enable** command disables dynamic EDCA parameter adjustment.

By default, dynamic EDCA parameter adjustment is disabled.

Format

dynamic-edca enable

undo dynamic-edca enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

A WLAN has only three non-overlapping channels on the 2.4 GHz frequency band. When APs are deployed densely, multiple APs have to work in the same channel, resulting in co-channel interference. This interference degrades network performance.

The dynamic EDCA parameter adjustment function allows APs to adjust EDCA parameters flexibly to reduce the possibility of collision, improve the throughput, and enhance user experience.

Example

Enable dynamic EDCA parameter adjustment.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] dynamic-edca enable
```

11.4.72 dynamic-edca threshold

Function

The **dynamic-edca threshold** command configures the threshold for the dynamic EDCA Best-Effort service.

The **undo dynamic-edca threshold** command restores the default threshold for the dynamic EDCA Best-Effort service.

The default threshold for the dynamic EDCA Best-Effort service is 6 pps.

Format

dynamic-edca threshold be-service *be-service-threshold*

undo dynamic-edca threshold be-service

Parameters

Parameter	Description	Value
be-service *be-service-threshold*	Specifies the threshold for the dynamic EDCA Best-Effort service.	The value is an integer that ranges from 1 to 1000, in pps.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When dynamic EDCA is enabled, the system dynamically adjusts EDCA parameters for the Best-Effort service and Background service based on the number of Best-Effort users, improving user experience.

If the number of Best-Effort service packets from a user in the radio's internal statistics queue exceeds the threshold (specified using the **dynamic-edca threshold** command) per unit time (1s), the user is considered a Best-Effort user.

Before running this command, you must run the **dynamic-edca enable** command to enable dynamic EDCA.

Example

Set the threshold for the dynamic EDCA Best-Effort service to 10 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] dynamic-edca enable
[HUAWEI-wlan-rrm-prof-default] dynamic-edca threshold be-service 10
```

11.4.73 sta-number gap-threshold

Function

The **sta-number gap-threshold** command sets the load difference threshold for load balancing based on the number of users in a static load balancing group.

The **undo sta-number gap-threshold** command restores the default load difference threshold for load balancing based on the number of users in a static load balancing group.

By default, the load difference threshold of a static load balancing group is specified based on the number of users, and the default value is 3.

Format

sta-number gap-threshold { **percentage** *percentage-value* | **number** *number-value* }

undo sta-number gap-threshold

Parameters

Parameter	Description	Value
percentage *percentage-value*	Specifies the load difference threshold for static load balancing based on the percentage of users.	The value is an integer that ranges from 1 to 100. It indicates the threshold of the load difference among radios in a load balancing group, in percentage. The load difference refers to the difference between the percentages of users on radios.
number *number-value*	Specifies the load difference threshold for static load balancing based on the number of users.	The value is an integer that ranges from 1 to 20. It indicates the threshold of the load difference among radios in a load balancing group. The load difference refers to the difference between the numbers of users on radios.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following load balancing algorithm is used after the user access to determine whether to steer the user to a new AP:

One of the conditions for steering a user to a new AP is that the radio of the target load is lower than that of the current access radio. The radio load is identified by the number or percentage (Number of users associated with the current radio/Maximum number of access users supported by the radio x 100%) of access users. If the load difference between the target radio and current radio exceeds the specified threshold, the condition is met.

Precautions

If you configure the load difference threshold based on both the number of users and the percentage of users, only the latest configuration takes effect.

Example

Set the load difference threshold for load balancing based on the percentage of users in the static load balancing group to 40%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] sta-number gap-threshold percentage 40
```

11.4.74 high-density amc-optimize enable

Function

The **high-density amc-optimize enable** command enables the adaptive modulation and coding (AMC) optimization function in high-density scenarios.

The **undo high-density amc-optimize enable** command disables the AMC optimization function in high-density scenarios.

By default, the AMC optimization function is disabled in high-density scenarios.

Format

high-density amc-optimize enable

undo high-density amc-optimize enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In typical high-density scenarios, a large number of hidden nodes exist, which interfere in communication between APs and STAs and affect product performance. The AMC optimization function can reduce such interference and improve the AMC algorithm performance.

- It is recommended that this function be enabled in high-density scenarios where directional antennas are used.
- This function is not applicable to scenarios where STAs move fast between APs.

Precautions

- The AMC optimization in high-density scenarios is not supported by the following APs:
  - AirEngine 9700D-S (including matching ORUs)
  - AirEngine X77X
  - AirEngine X76X
- This function does not take effect in MU-MIMO mode.

Example

Enable the AMC optimization function in high-density scenarios on the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] high-density amc-optimize enable
```

11.4.75 interference adjacent-channel threshold

Function

The **interference adjacent-channel threshold** command configures the alarm threshold for adjacent-channel interference.

The **undo interference adjacent-channel threshold** command restores the default alarm threshold for adjacent-channel interference.

By default, the alarm threshold for adjacent-channel interference is 50%.

Format

interference adjacent-channel threshold *threshold-value*

undo interference adjacent-channel threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold, which is the percentage of the adjacent-channel interference power against the maximum power.	The value is an integer that ranges from 1 to 100, in percentage.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Two APs with different center frequencies have overlapping areas, resulting in adjacent-channel interference. When APs are placed too close to each other or have strong signals, more noise is produced, degrading network performance.

After the **interference detect-enable** command is executed to enable interference detection, an AP can detect adjacent-channel interference. When the AP detects that adjacent-channel interference exceeds the alarm threshold configured using the **interference adjacent-channel threshold** command, the AP sends an alarm to the AC.

Example

Set the alarm threshold for adjacent-channel interference to 52%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio0
[HUAWEI-wlan-radio-2g-prof-radio0] interference detect-enable
[HUAWEI-wlan-radio-2g-prof-radio0] interference adjacent-channel threshold 52
```

11.4.76 interference co-channel threshold

Function

The **interference co-channel threshold** command configures the alarm threshold for co-channel interference.

The **undo interference co-channel threshold** command restores the default alarm threshold for co-channel interference.

By default, the alarm threshold for co-channel interference is 50%.

Format

interference co-channel threshold *threshold-value*

undo interference co-channel threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold, which is the percentage of the co-channel interference power against the maximum power.	The value is an integer that ranges from 1 to 100, in percentage.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Two APs working in the same frequency band interfere with each other. For example, on a large-scale WLAN (a university campus network), different APs often use the same channel. When there are overlapping areas among these APs, co-channel interference exists, degrading network performance.

After the **interference detect-enable** command is executed to enable interference detection, an AP can detect adjacent-channel interference. When the AP detects that co-channel interference exceeds the alarm threshold configured using the **interference co-channel threshold** command, the AP sends an alarm to the AC.

Example

Set the alarm threshold for co-channel interference to 60%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio0
[HUAWEI-wlan-radio-2g-prof-radio0] interference detect-enable
[HUAWEI-wlan-radio-2g-prof-radio0] interference co-channel threshold 60
```

11.4.77 interference detect-enable

Function

The **interference detect-enable** command enables interference detection.

The **undo interference detect-enable** command disables interference detection.

By default, interference detection is disabled.

Format

interference detect-enable

undo interference detect-enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

WLAN wireless channels are vulnerable to interference in surrounding radio environments, and the service quality is therefore degraded. If interference detection is configured, a monitor AP can know the radio environment in real time and report alarms to the AC in a timely manner.

Interference detection enables an AP to detect AP co-channel interference, AP adjacent-channel interference, and STA interference.

- AP co-channel interference: Two APs working on the same frequency band interfere with each other. For example, on a large-scale WLAN (a university campus network), different APs often use the same channel. When there are overlapping areas among these APs, co-channel interference exists, degrading network performance.
- AP adjacent-channel interference: Two APs with different center frequencies have overlapping areas, resulting in adjacent-channel interference. Therefore, if APs are placed too close to each other or they have strong signals, more noise will be produced, degrading network performance.
- STA interference: If there are many STAs that are managed by other APs around an AP, services of the STAs managed by the local AP may be affected.

Example

Enable interference detection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio0
[HUAWEI-wlan-radio-2g-prof-radio0] interference detect-enable
```

11.4.78 interference station threshold

Function

The **interference station threshold** command configures the alarm threshold for STA interference.

The **undo interference station threshold** command restores the default alarm threshold for STA interference.

By default, the alarm threshold for STA interference is 32.

Format

interference station threshold *threshold-value*

undo interference station threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold.	The value is an integer that ranges from 1 to 256.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

If there are many STAs that are managed by other APs around an AP, services of the STAs managed by the local AP may be affected.

After the **interference detect-enable** command is executed to enable interference detection, an AP can detect STAs that are managed by other APs. When the AP detects that the number of such STAs exceeds the alarm threshold configured using the **interference station threshold** command, the AP sends an alarm to the AC.

Example

Set the alarm threshold for STA interference to 50.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio0
[HUAWEI-wlan-radio-2g-prof-radio0] interference station threshold 50
```

11.4.79 interference-visualization enable

Function

The **interference-visualization enable** command enables interference visualization on AP radios.

The **undo interference-visualization enable** command disables interference visualization on AP radios.

By default, interference visualization is disabled on AP radios.

NOTE

Interference visualization is not available for the following models:

- AirEngine x761
- AirEngine x762

Format

interference-visualization enable

undo interference-visualization enable

Parameters

None

Views

AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the AP is connected to an analyzer, you can enable interference visualization on radios of co-channel APs so that packet transmission information on the co-channel APs can be displayed on the analyzer, thereby showing air interface interference behavior.

Pre-configuration Tasks

Configure KPI reporting, and run the **ap log module mid** *ffdc0000* command in the WMI profile view to report logs of the interference visualization module to the analyzer.

Precautions

Interference visualization can be enabled on a maximum of 20 AP radios. To view information about all AP radios on which interference visualization is enabled, run the **display interference-visualization configuration** command.

Example

Enable interference visualization on radio 1 of AP 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 1
[HUAWEIwlan-radio-1/1] interference-visualization enable
```

11.4.80 member (static load balancing group view)

Function

The **member** command adds an AP radio to a static load balancing group.

The **undo member** command deletes an AP radio from a load balancing group.

By default, no AP radio is added to a static load balancing group.

Format

member { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }&<1-16>

undo member { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }&<1-16>

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of an AP. The AP name and radio ID identify a radio.	The AP name must exist.
ap-id *ap-id*	Specifies the ID of an AP. The AP ID and radio ID identify a radio.	The AP ID must exist.
radio *radio-id*	Specifies a radio ID. The radio ID and AP name identify a radio.	The radio ID must exist.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to add an AP radio to or delete an AP radio from a static load balancing group. When a STA requests to connect to an AP radio in a static load balancing group, the AC compares the load of the radio and other working radios in the load balancing group and determines whether to allow the STA to connect to the radio according to a load balancing algorithm.

Precautions

- If dual-band APs are used, traffic is load balanced among APs working on the same frequency band.
- Each load balancing group supports a maximum of 16 AP radios.
- Under the agile distributed network architecture, you only need to add radios of the RUs to a static load balancing group. Central APs are not supported in static load balancing groups.
- A radio configured with channel 184, 188, 192, or 196 on the 4.9 GHz frequency band cannot be used for load balancing.

Example

Add radio 0 of AP **office** to the static load balancing group **coco**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] member ap-name office radio 0
```

11.4.81 power auto-adjust enable

Function

The **power auto-adjust enable** command enables signal-strength-based power adjustment for APs.

The **undo power auto-adjust enable** command disables signal-strength-based power adjustment for APs.

By default, signal-strength-based power adjustment is disabled for an AP.

NOTE

This command does not take effect for the following APs:

- AirEngine X77X
- AirEngine X76X

Format

power auto-adjust enable

undo power auto-adjust enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traditional radio power control function sets the power of an AP to a fixed value to keep the power of all STAs connecting to the AP the same.

You can run the **power auto-adjust enable** command to enable signal-strength-based power adjustment. This function enables an AP to detect the signal strength of a STA in a timely manner. If the AP detects that the signal strength of the STA is strong (for example, the STA is near the AP), the AP reduces its transmit power

when sending packets. If the AP detects that the signal strength of the STA is weak (for example, the STA is far from the AP), the AP uses the normal transmit power to send radio signals.

Prerequisites

The power mode has been set to automatic using the **calibrate auto-txpower-select enable** command.

Example

Enable signal-strength-based power adjustment for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] power auto-adjust enable
```

11.4.82 radio-reload time-range

Function

The **radio-reload time-range** command enables scheduled radio reloading on APs.

The **undo radio-reload time-range** command disables scheduled radio reloading on APs.

By default, scheduled radio reloading is disabled on APs.

Format

radio-reload time-range *time-range*

undo radio-reload time-range

Parameters

Parameter	Description	Value
time-range	Specifies a time range during which radios are reloaded as scheduled.	The specified time range must exist.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After APs run for a long time, some unknown exceptions may occur. You can run this command to configure a scheduled policy for APs to reload radios during off-peak hours. This prevents potential exceptions or addresses existing exceptions.

Prerequisites

A time range for scheduled radio reloading has been specified by using the **time-range** command.

Precautions

After scheduled radio reloading is configured, APs reload radios in batches within the specified time range. During radio reloading on an AP, STAs associated with the AP are steered to neighboring APs. To prevent impact on services, it is recommended that radio reloading be performed during a time range when no service traffic is transmitted.

This function is not recommended in industrial scenarios where services need to run continuously for a long time.

Example

Enable the scheduled radio reloading function for 5 GHz radios of APs and specify the time range of 01:00 to 05:00 every day for scheduled radio reloading.

```
<HUAWEI> system-view
[HUAWEI] time-range test 01:00 to 05:00 daily
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name wlan-radio5g
[HUAWEI-wlan-radio-5g-prof-wlan-radio5g] radio-reload time-range test
```

11.4.83 reset ap traffic statistics wireless

Function

The **reset ap traffic statistics wireless** command clears packet statistics on a specified AP radio.

Format

reset ap traffic statistics wireless { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Clears packet statistics on the AP with a specified name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Clears packet statistics on the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Clears packet statistics on a specified radio.	The radio ID must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to clear packet statistics on a specified AP radio.

Example

Clear packet statistics on radio 2 of the AP with the ID 0.

```
<HUAWEI> reset ap traffic statistics wireless ap-id 0 radio 2
```

11.4.84 reset station steer-history

Function

The **reset station steer-history** command deletes historical information about STA migrations.

Format

reset station steer-history

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to delete historical information about STA migrations.

Example

Delete historical information about migrations of all STAs.
<HUAWEI> **reset station steer-history**

11.4.85 reset flexible-radio switch-record

Function

The **reset flexible-radio switch-record** command clears switching records of redundant radios.

Format

reset flexible-radio switch-record all

Parameters

Parameter	Description	Value
all	Clears switching records of all redundant radios.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **reset flexible-radio switch-record** command to clear switching records of redundant radios.

Example

Clear switching records of all redundant radios.
<HUAWEI> **reset flexible-radio switch-record all**

11.4.86 reset station steer-statistics

Function

The **reset station steer-statistics** command deletes statistics about STA steering.

Format

reset station steer-statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to delete statistics about STA steering.

Example

Delete statistics about STA steering.
<HUAWEI> **reset station steer-statistics**

11.4.87 reset wlan calibrate statistics

Function

The **reset wlan calibrate statistics** command clears radio calibration statistics.

Format

reset wlan calibrate statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Clears radio calibration statistics on the AP with the specified AP name. The AP name and radio ID together identify a radio.	The AP name must exist.
ap-id *ap-id*	Clears radio calibration statistics on the AP with the specified AP ID. The AP ID and radio ID together identify a radio.	The AP ID must exist.

Parameter	Description	Value
radio *radio-id*	Clears calibration statistics about the radio with the specified radio ID. The radio ID and AP name together identify a radio.	The radio ID must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Run the **reset wlan calibrate statistics** command to clear radio calibration statistics, including the number of times the radio environment deteriorates and number of times the radio channel and power are calibrated.

Example

Clear calibration statistics about radio 0 on AP0.

```
<HUAWEI> reset wlan calibrate statistics ap-id 0 radio 0
```

11.4.88 rrm-profile (WLAN view)

Function

The **rrm-profile** command creates an RRM profile and displays the RRM profile view.

The **undo rrm-profile** command deletes an RRM profile.

By default, the system provides the RRM profile **default**.

Format

rrm-profile name *profile-name*

undo rrm-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an RRM profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all RRM profiles.	The RRM profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WLAN technology uses radio signals (such as 2.4 GHz or 5 GHz radio waves) as transmission medium. Radio signals will attenuate when transmitted over the air, degrading service quality for wireless users. Radio resource management (RRM) enables a WLAN to adapt to changes in the radio environment by dynamically adjusting radio resources. This improves service quality for wireless users.

Follow-up Procedure

Run the **rrm-profile (radio profile view)** command to bind the RRM profile to a radio profile so that the RRM profile can take effect.

Example

Create the RRM profile **rrm01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name rrm01
[HUAWEI-wlan-rrm-prof-rrm01]
```


11.4.89 rrm-profile (radio profile view)

Function

The **rrm-profile** command binds an RRM profile to a radio profile.

The **undo rrm-profile** command unbinds an RRM profile from a radio profile.

By default, the RRM profile **default** is bound to a radio profile.

Format

rrm-profile *profile-name*

undo rrm-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an RRM profile.	The RRM profile name must already exist.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After you create an RRM profile using the **rrm-profile (WLAN view)** command, bind the RRM profile to a radio profile so that the RRM profile can take effect.

Example

Bind the RRM profile **rrm01** to the radio profile **office01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name rrm01
[HUAWEI-wlan-rrm-prof-rrm01] quit
[HUAWEI-wlan-view] radio-2g-profile name office01
[HUAWEI-wlan-radio-2g-prof-office01] rrm-profile rrm01
```

11.4.90 rssi-diff-gap

Function

The **rssi-diff-gap** command sets the RSSI difference threshold for members in a static load balancing group.

The **undo rssi-diff-gap** command restores the default RSSI difference threshold of members in a static load balancing group.

By default, the RSSI difference threshold of members in a static load balancing group is 5 dB.

Format

rssi-diff-gap *diff-gap-threshold*

undo rssi-diff-gap

Parameters

Parameter	Description	Value
diff-gap-threshold	Specifies the RSSI difference threshold of members in a static load balancing group.	The value is an integer that ranges from 0 to 15, in dB.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To achieve load balancing, an AP may steer connected STAs to other APs with smaller RSSIs. If the RSSI of the AP with which a STA currently associates minus the RSSI of the target AP is larger than the specified RSSI difference threshold, the STA is denied from being steered to the target AP; otherwise, the STA can be steered to the target AP.

Precautions

If STAs have high signal quality deterioration tolerance for the target AP, you can set a larger RSSI difference threshold to achieve better load balancing effect. If STAs have low signal quality deterioration tolerance for the target AP, set a smaller RSSI difference threshold. You are advised to retain the default value.

Example

Set the RSSI difference threshold for members in a static load balancing group to 6 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] rssi-diff-gap 6
```


11.4.91 rssi-threshold

Function

The **rssi-threshold** command sets an RSSI threshold for member devices in a static load balancing group.

The **undo rssi-threshold** command restores the default RSSI threshold of member devices in a static load balancing group.

By default, the RSSI threshold of member devices in a static load balancing group is –65 dBm.

Format

rssi-threshold *rssi-threshold*

undo rssi-threshold

Parameters

Parameter	Description	Value
rssi-threshold	Specifies the RSSI threshold of members in a static load balancing group.	The value is an integer that ranges from –75 to –55, in dBm.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting an RSSI threshold for member devices in a static load balancing group is to filter APs with weak signals, so that STAs can be load balanced between APs with better signals. This prevents STAs from associating with APs with weak signals but light loads. This function does not affect STAs' going online.

Example

Set the RSSI threshold for member devices in a static load balancing group to –70 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] rssi-threshold -70
```


11.4.92 rx-sensitivity

Function

The **rx-sensitivity** command sets the receiver sensitivity threshold of an AP.

The **undo rx-sensitivity** command restores the default receiver sensitivity threshold of an AP.

By default, the receiver sensitivity threshold of an AP is –128 dBm.

Format

rx-sensitivity *threshold*

undo rx-sensitivity

Parameters

Parameter	Description	Value
threshold	Specifies the receiver sensitivity threshold of an AP.	The value is an integer that ranges from –128 to –40, in dBm.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The sensitivity threshold can be used to adjust the anti-interference capability of radios.

Precautions

The receiver sensitivity threshold cannot be set higher than the upper AGC threshold.

Modifying the receiver sensitivity threshold will affect the uplink access coverage or user access. It is recommended that the default setting be remained or the threshold be modified under the guidance of professional technical personnel.

Example

Set the receiver sensitivity threshold to –70 dBm in the 2G radio profile **test**.

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



```
[HUAWEI-wlan-view] radio-2g-profile name test
[HUAWEI-wlan-radio-2g-prof-test] rx-sensitivity -70
Warning: This parameter will affect the uplink access coverage or user access. I
t is recommended that the configuration be modified under the guidance of profes
sional technical personnel. Continue? [Y/N]:y
```

11.4.93 scan-channel-set

Function

The **scan-channel-set** command configures an air scan channel set.

The **undo scan-channel-set** command restores the default air scan channel set.

By default, an air scan channel set contains all channels supported by the country code of an AP.

Format

scan-channel-set { **country-channel** | **dca-channel** | **work-channel** }

undo scan-channel-set

Parameters

Parameter	Description	Value
country-channel	Specifies an air scan channel set that contains all channels supported by the country code of an AP.	-
dca-channel	Specifies a calibration channel set as the air scan channel set. To configure a calibration channel set, run the **dca-channel channel-set** command.	-
work-channel	Specifies an air scan channel set that contains working channels of APs.	-

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **scan-channel-set** command to specify an air scan channel set for an AP, the AP scans channels in the channel set. The collected information is reported to the AC or server for radio calibration, smart roaming, spectrum analysis, WLAN location, or WIDS data analysis.

Precautions

- If the air scan channel set you specified contains all channels supported by the country code of the AP, the AP scans data on many channels but the channel scanning lasts for a long time, which may affect real-time data analysis.
- If you specify a calibration channel set as the air scan channel set, the AP scans data on a few channels. This reduces the channel scanning time, increases the terminal location accuracy, and reduces burden on the device.
- If you add only working channels of an AP to the air scan channel set, the AP only scans the working channels.

Example

Configure an air scan channel set that contains all calibration channels.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-channel-set dca-channel
```

11.4.94 scan-disable

Function

The **scan-disable** command disables the air scan function.

The **undo scan-disable** command enables the air scan function.

By default, the air scan function is enabled.

Format

scan-disable

undo scan-disable

Parameters

None

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP does not require air scan, you can run the **scan-disable** command to disable the air scan function. The AP then will stop scanning surrounding wireless signals.

Precautions

Disabling air scan will affect scanning functions, such as radio calibration, spectrum analysis, terminal location, WIDS, smart roaming, and DFS smart selection.

Example

Disable the air scan function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-disable
Warning: This operation will affect scanning-related services such as radio calibration, spectrum analysis, terminal location, WIDS
function, smart roaming and DFS smart selection.Continue? [Y/N]y
```

11.4.95 scan-enhancement

Function

The **scan-enhancement** command enables the scanning enhancement function.

The **undo scan-enhancement** command disables the scanning enhancement function.

By default, the scanning enhancement function is disabled.

NOTICE

The scanning enhancement function is supported only by the AirEngine 6761-21, AirEngine 6761-21E, and AirEngine 6761S-21.

Format

scan-enhancement

undo scan-enhancement

Parameters

None

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

The third radio of some APs is used specifically for radio scanning and does not support configuration or STA access. After the scanning enhancement function is

enabled, the current radio works with the third radio to perform radio scanning and provide scanning feature data. When multiple radios collect and provide data simultaneously, the scanning performance and precision are improved. After the scanning enhancement function is disabled, scanning feature data on the current radio is provided by the third radio. The third radio does not involve in scanning. Therefore, scanning features on the radio do not affect STA access.

The third radio of these APs supports scanning only on the single spatial stream. When functions such as location and WIDS detection, it is recommended that the scanning enhancement function be enabled if high performance and precision are required.

When services that are sensitive to packet loss or delay (for example, voice or video services) are used, it is recommended that the scanning enhancement function be disabled.

Example

Enable the scanning enhancement function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-enhancement
```

11.4.96 scan-interval

Function

The **scan-interval** command sets an air scan interval.

The **undo scan-interval** command restores the default air scan interval.

By default, the air scan interval is 10000 ms.

Format

scan-interval *scan-time*

undo scan-interval

Parameters

Parameter	Description	Value
scan-time	Specifies an air scan interval. With a smaller air scan interval, more sampling data can be obtained, which increases the performance overhead in turn. An air scan interval of less than 2000 ms may affect service running.	The value is an integer that ranges from 300 to 600000, in milliseconds.

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an air scan interval is specified using the **scan-interval** command, APs scan channels at the specified intervals.

When spectrum analysis is used, the air scan interval range of 3s to 10s and the air scan period of 100 ms are recommended. This helps you obtain sufficient sampled data without compromising normal services.

Precautions

The air scan interval also applies to radio calibration, smart roaming, spectrum analysis, WLAN location, and WIDS functions.

If the customer has high requirements on real-time data analysis, configure a small air scan interval using the **scan-interval** command to improve the scan frequency. However, higher scan frequency indicates much larger impact on the services.

Ensure that the air scan interval meets the following condition: scan-interval ≥ beacon-interval + 100 ms

In vehicle-ground communication scenarios, the air scan interval ranges from 300 ms to 1000 ms.

Example

Set the air scan interval to 3000 ms for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-interval 3000
```

11.4.97 scan-period

Function

The **scan-period** command sets the air scan period.

The **undo scan-period** command restores the default air scan period.

By default, the air scan period is 60 ms.

Format

scan-period *scan-time*

undo scan-period

Parameters

Parameter	Description	Value
scan-time	Specifies the air scan period.	The value is an integer that ranges from 60 to 100, in milliseconds.

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the air scan period is configured using the **scan-period** command, an AP continuously scans surrounding radio signals in the configured period. After the period expires, the AP reports the collected information to an AC or server. The information is used for radio calibration, smart roaming, spectrum analysis, WLAN location, or WIDS data analysis.

When spectrum analysis is used, the air scan interval range of 3s to 10s and the air scan period of 100 ms are recommended. This helps you obtain sufficient sampled data without compromising normal services.

Precautions

A longer air scan period indicates more collected data and a more accurate data analysis result. However, if the air scan period is set too large, WLAN services are affected. You are advised to use the default value.

Example

Set the air scan period to 80 ms for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-period 80
```

11.4.98 scene

Function

The **scene** command binds a scenario profile to an AP group or a single AP.

The **undo scene** command unbinds a scenario profile from an AP group or a single AP.

By default, no scenario profile is bound to an AP group or a single AP.

Format

scene *scene-name*

undo scene

Parameters

Parameter	Description	Value
scene-name	Specifies the name of a scenario profile.	The value is of the enumerated type. ● multi-partition-cross-room: indicates an indoor multi-partition cross-room deployment scenario (capacity first). ● multi-partition-cross-room-cov: indicates an indoor multi-partition cross-room deployment scenario (coverage first). ● automated-guided-vehicle: indicates an AGV scenario. ● high-density-stadium: indicates a high-density stadium scenario. ● indoor-high-density: indicates an indoor high-density coverage scenario. ● indoor-low-density: indicates an indoor low-density coverage scenario. ● indoor-multi-partition: indicates an indoor multi-partition coverage scenario. ● indoor-normal-density: indicates an indoor common coverage scenario. ● industrial-manufacturing: indicates an industrial manufacturing scenario. ● outdoor-continuous: indicates an outdoor continuous coverage scenario.

Parameter	Description	Value
		• virtual-reality: indicates a VR scenario.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In actual scenarios, there are fixed recommended settings for radio parameters such as the channel, bandwidth, and transmit power. Recommended settings for these typical scenarios are configured into scenario profiles. When configuring wireless services, you only need to bind a scenario profile to an AP group or a single AP, greatly simplifying service configuration.

To view the parameter settings in preset scenario profiles, run the **display wlan scene** command. If the value of a parameter is empty, a hyphen (-) is displayed, indicating that the parameter is not configured.

Precautions

- The service parameters on an AP take effect in the following sequence: Parameters in the scenario profile bound to an AP > Parameters directly configured for an AP > Parameters in the scenario profile identified and delivered by the analyzer to an AP > Parameters in the scenario profile bound to the AP group to which the AP belongs > Parameters directly configured for the AP group to which the AP belongs.

  The calibration bandwidth of the 5 GHz frequency band is used as an example. Assume that the parameter value in a scenario profile **a** bound to the AP is empty, the parameter value in scenario profile **b** bound to the AP group is **B**, the parameter value corresponding to scenario profile **c** identified and delivered by the analyzer to the AP is **C**, the parameter value configured for an AP is **D**, and the parameter value configured for an AP group is **E**. Then the parameter value takes effect on the AP in the following sequence: null > **D** > **C** > **B** > **E**. That is, the parameter value that takes effect is **D**.
- The wireless service parameters in a scenario profile contain the radio calibration parameter set (**Radio calibration**). After a scenario profile is configured, the radio calibration parameter settings take effect from the next radio calibration.
- Although a series of radio calibration parameters are predefined in a scenario profile, the channel, bandwidth, and transmit power are still restricted by the country code during radio calibration. Bandwidth selection depends on the number of channels allowed by the country code.

Assume that the calibration bandwidth defined in the scenario profile is A, the number of available channels under this bandwidth is B in the country code, and the calibration bandwidth configured in the regulatory domain profile is C.

- If B is greater than or equal to 3, the calibration bandwidth A takes effect.
- If B is smaller than 3, the smaller value between A and C is used as the calibration bandwidth.

Example

Bind the scenario profile **multi-partition-cross-room** to the AP group **mygroup**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name mygroup
[HUAWEI-wlan-ap-group-mygroup] scene multi-partition-cross-room
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.4.99 smart-antenna { enable | disable }

Function

The **smart-antenna** { **enable** | **disable** } command enables or disables the smart antenna selection algorithm for an AP.

The **undo smart-antenna** command restores the smart antenna selection algorithm of an AP to the default state.

By default, the smart antenna selection algorithm is enabled.

Format

smart-antenna { **enable** | **disable** }

undo smart-antenna

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the smart antenna selection algorithm, an AP can adjust the antenna mode for transmitting signals based on STA locations and select a proper combination of

antenna arrays to communicate with STAs. This improves the RSSIs of STAs and improves user experience.

Precautions

The smart antenna selection algorithm is supported only by the following APs:

- AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 5760-51, AirEngine 6760-X1, and AirEngine 8760-X1-PRO

Example

Enable the smart antenna selection algorithm for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna enable
```

11.4.100 smart-antenna throughput-triggered-training

Function

The **smart-antenna throughput-triggered-training** command sets a sudden performance change threshold that triggers smart antenna training.

The **undo smart-antenna throughput-triggered-training** command restores the default sudden performance change threshold that triggers smart antenna training.

The default sudden performance change threshold that triggers smart antenna training is 10%.

Format

smart-antenna throughput-triggered-training threshold *threshold*

undo smart-antenna throughput-triggered-training threshold

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies a sudden performance change threshold that triggers antenna training.	The value is an integer that ranges from 10 to 50, in percentage. In addition, the value must be a multiple of 10.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In a smart antenna system, the device monitors performance (throughput) of transmit ends. If the detected throughput of a transmit end exceeds the sudden performance change threshold specified using the **smart-antenna throughput-triggered-training** command, a new round of antenna training is triggered.

- In a good air interface environment, set a high sudden performance change threshold to prevent frequent antenna training from affecting user services.
- In a poor air interface environment, set a low sudden performance change threshold to improve the WLAN's anti-interference capability.

Example

Set the sudden performance change threshold that triggers antenna training to 10%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna throughput-triggered-training threshold 10
```

11.4.101 smart-antenna training-interval

Function

The **smart-antenna training-interval** command sets the smart antenna training interval.

The **undo smart-antenna training-interval** command restores the default smart antenna training interval.

The default smart antenna training interval is **auto**, indicating that a smart antenna is trained in self-adaptation mode.

Format

smart-antenna training-interval { *training-interval* | **auto** }

undo smart-antenna training-interval

Parameters

Parameter	Description	Value
training-interval	Indicates the smart antenna training interval.	The value is an integer that ranges from 10 to 600, in seconds.

Parameter	Description	Value
auto	Indicates that a smart antenna is trained in self-adaptation mode.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **smart-antenna training-interval** command to set the smart antenna training interval. When the period since the last round of smart antenna training exceeds the specified interval, a new round of smart antenna training is triggered.

Configure the smart antenna training interval based on actual situations.

- A short antenna training interval causes frequency antenna training and affects user services.
- A long antenna training interval causes the device's failure to switch the antenna combination in time to adapt to WLAN environment changes.

When the default smart antenna training interval is restored, that is, smart antennas are trained in self-adaptation mode, the device adaptively calculates the antenna training interval based on the number of concurrent STAs.

Example

Set the smart antenna training interval to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna training-interval 100
```

11.4.102 smart-antenna training-mpdu-number

Function

The **smart-antenna training-mpdu-number** command sets the number of MAC protocol data units (MPDUs) sent by an AP to a STA during smart antenna training.

The **undo smart-antenna training-mpdu-number** command restores the default number of MPDUs sent by an AP to a STA during smart antenna training.

By default, 640 MPDUs are sent by an AP to a STA during smart antenna training.

Format

smart-antenna training-mpdu-number *training-mpdu-number*

undo smart-antenna training-mpdu-number

Parameters

Parameter	Description	Value
training-mpdu-number	Specifies the number of MPDUs sent by an AP to a STA during smart antenna training.	The value is an integer that ranges from 10 to 1000.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In the smart antenna algorithm, an AP uses different antenna combinations to send training packets for antenna training. During smart antenna training, the transmit end (AP) sends training packets to a receive end (STA). The receive end measures the PER and RSSI in the received packets, and then sends the PER and RSSI to the transmit end. The transmit end collects information about all antenna combinations and corresponding PERs and RSSIs to determine the optimal antenna combination for the receiver.

You can run the **smart-antenna training-mpdu-number** command to set the number of MPDUs sent by an AP to a STA during smart antenna training.

If the traffic rate, bandwidth, and air interface rate of the STA are high, set a small value. Otherwise, set a large value.

Example

Set the number of MPDUs sent by an AP to a STA during smart antenna training to 600.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna training-mpdu-number 600
```

11.4.103 smart-antenna valid-per-scope

Function

The **smart-antenna valid-per-scope** command sets the upper and lower valid packet error rate (PER) thresholds in the smart antenna algorithm.

The **undo smart-antenna valid-per-scope** command restores the default upper and lower valid PER thresholds in the smart antenna algorithm.

The default upper and lower valid PER thresholds are 80% and 20%, respectively.

Format

smart-antenna valid-per-scope { **high-per-threshold** *high-per-threshold* | **low-per-threshold** *low-per-threshold* }

undo smart-antenna valid-per-scope { **high-per-threshold** | **low-per-threshold** }

Parameters

Parameter	Description	Value
high-per-threshold *high-per-threshold*	Specifies the upper valid PER threshold.	The value is an integer that ranges from 50 to 90, in percentage. In addition, the value must be a multiple of 10.
low-per-threshold *low-per-threshold*	Specifies the lower valid PER threshold.	The value is an integer that ranges from 10 to 30, in percentage. In addition, the value must be a multiple of 10.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In the smart antenna algorithm, an AP uses different antenna combinations to send training packets for antenna training. During smart antenna training, the transmit end (AP) sends training packets to a receive end (STA). The receive end measures the PER and RSSI in the received packets, and then sends the PER and RSSI to the transmit end. The transmit end collects information about all antenna combinations and corresponding PERs and RSSIs to determine the optimal antenna combination for the receiver.

The PER is a key basis for the smart antenna algorithm. After proper upper and lower valid PER thresholds are configured, the smart antenna algorithm can select

a proper antenna combination to improve the coverage and anti-interference capability of a WLAN in indoor coverage scenarios.

Example

Set the upper valid PER threshold to 80%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna valid-per-scope high-per-threshold 80
```

11.4.104 smart-roam advanced-scan disable

Function

The **smart-roam advanced-scan disable** command disables coordinated scanning in roaming.

The **undo smart-roam advanced-scan disable** command enables coordinated scanning in roaming.

By default, coordinated scanning in roaming is enabled.

Format

smart-roam advanced-scan disable

undo smart-roam advanced-scan disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the roaming steering for sticky STAs, real-time information about neighboring APs is required to determine the target AP. If STAs do not support 802.11k radio resource measurement, you can run the **undo smart-roam advanced-scan disable** command to enable coordinated scanning in roaming. In this way, APs can collect real-time information about neighboring APs through synchronized radio resource measurement, and generate a neighbor AP table of the STAs.

After this function is enabled, radios switch channels to scan STA information while ensuring voice and video services. If voice and video services are affected, you can disable this function.

Prerequisites

The smart roaming or AI roaming function has been enabled.

Example

Enable coordinated scanning in roaming.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] undo smart-roam advanced-scan disable
```

11.4.105 smart-roam { disable | enable | ai-mode }

Function

The **smart-roam { disable | enable | ai-mode }** command enables or disables AI roaming and smart roaming.

The **undo smart-roam** command restores the default state of AI roaming and smart roaming.

By default, AI roaming and smart roaming are enabled.

Format

smart-roam { **disable** | **enable** | **ai-mode** }

undo smart-roam

Parameters

Parameter	Description	Value
disable	Disables AI roaming and smart roaming.	-
enable	Enables smart roaming and disables AI roaming.	-
ai-mode	Enables AI roaming and smart roaming.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a traditional WLAN, when a STA is farther from an AP, the access rate of the STA becomes lower but the STA still associates with the AP without reconnecting the AP or roaming to another AP. This degrades user experience. After the smart roaming function is enabled, when an AP detects that the SNR or access rate of a STA is lower than the specified threshold, the AP sends a BTM packet or Disassociation packet to the STA. The STA then reconnects to the network or roams to an AP with stronger signals.

In practice, the roaming process depends on multiple negotiations between APs and STAs. STAs of different vendors and models have different autonomous behaviors during the negotiation process. As a result, roaming experience cannot be effectively guaranteed. To address this issue, you can enable the AI roaming function. Then the system matches the identified terminal type with the corresponding terminal profile to obtain the behavior characteristics of the terminal during roaming and perform optimization during roaming negotiation. This improves the roaming sensitivity and success rate, enhancing the roaming experience of users.

NOTE

Before enabling the AI roaming function, enable the terminal identification 2.0 function and terminal profiling functions.

If the PMF function is enabled, the AI roaming function does not take effect.

APs must support independent radio scanning to achieve roaming steering based on coordinated measurement. For APs that do not support independent radio scanning, after the AI roaming function is enabled, the STA profiling mechanism is used to perform personalized roaming steering for STAs based on the triggering logic of smart roaming.

Follow-up Procedure

Run the **smart-roam roam-threshold { check-snr | check-rate }** command to configure the trigger mode of smart roaming and the **smart-roam roam-threshold { snr | rate }** command to configure the smart roaming threshold. After that, APs forcibly disconnect STAs with SNR or access rate lower than the threshold.

Example

Enable smart roaming.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
```

11.4.106 smart-roam quick-kickoff back-off-time

Function

The **smart-roam quick-kickoff back-off-time** command sets the backoff time for quickly disconnecting STAs.

The **undo smart-roam quick-kickoff back-off-time** command restores the default backoff time for quickly disconnecting STAs.

By default, the backoff time for quickly disconnecting STAs is 60 seconds.

Format

smart-roam quick-kickoff back-off-time *back-off-time*

undo smart-roam quick-kickoff back-off-time

Parameters

Parameter	Description	Value
back-off-time	Specifies the backoff time for quickly disconnecting STAs.	The value is an integer that ranges from 1 to 600, in seconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of quickly disconnecting STAs is enabled, you can run the **smart-roam quick-kickoff back-off-time** command to set the backoff time for quickly disconnecting STAs to prevent STAs from being disconnected frequently. STAs are not disconnected within the backoff time.

Precautions

Do not set the backoff time to a too small value. Otherwise, STAs may be disconnected frequently.

Example

Set the backoff time for quickly disconnecting STAs to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff back-off-time 60
```


11.4.107 smart-roam quick-kickoff-threshold disable

Function

The **smart-roam quick-kickoff-threshold disable** command disables the function of quickly disconnecting STAs.

The **undo smart-roam quick-kickoff-threshold disable** command enables the function of quickly disconnecting STAs.

By default, the function of quickly disconnecting STAs is enabled.

Format

smart-roam quick-kickoff-threshold disable

undo smart-roam quick-kickoff-threshold disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of quickly disconnecting STAs is enabled and the threshold for quickly disconnecting STAs is specified, the AP disconnects STAs whose SNR or access rate is lower than the specified threshold. The STAs then can connect to or roam to another AP with stronger signals.

Follow-up Procedure

Run the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command to set the mode for triggering the function of quickly disconnecting STAs, and the **smart-roam quick-kickoff-threshold** command to set the threshold for quickly disconnecting STAs. The AP will disconnect STAs whose SNR or access rate is lower the specified threshold.

Example

Enable the function of quickly disconnecting STAs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
```


11.4.108 smart-roam quick-kickoff-threshold { check-snr | check-rate }

Function

The **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command sets the mode for triggering the function of quickly disconnecting STAs.

The **undo smart-roam quick-kickoff-threshold** command restores the default mode for triggering the function of quickly disconnecting STAs.

The default mode for triggering the function of quickly disconnecting STAs is **check-snr**.

Format

smart-roam quick-kickoff-threshold { **check-snr** | **check-rate** } *

undo smart-roam quick-kickoff-threshold

Parameters

Parameter	Description	Value
check-snr	Specifies that the function of quickly disconnecting STAs is triggered by checking the SNR of STAs.	-
check-rate	Specifies that the function of quickly disconnecting STAs is triggered by checking the rate of STAs. The rate here refers to the negotiated rate based on the protocol and signal strength when a STA associates with an AP, instead of the actual rate of the STA.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of quickly disconnecting STAs is enabled, you can run the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command to set the mode for triggering the function of quickly disconnecting STAs, and set the threshold for quickly disconnecting STAs. When the SNR or access rate of a STA

detected by an AP is lower than the specified threshold, the AP disconnects the STA. The STA then can connect to or roam to another AP with stronger signals.

Prerequisites

The function of quickly disconnecting STAs has been enabled using the **undo smart-roam quick-kickoff-threshold disable** command.

Follow-up Procedure

Run the **smart-roam quick-kickoff-threshold** command to set the threshold for quickly disconnecting STAs.

Example

Set the mode for triggering the function of quickly disconnecting STAs to **check-rate**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold check-rate
```

11.4.109 smart-roam quick-kickoff-snr check-interval

Function

The **smart-roam quick-kickoff-snr check-interval** command configures the interval for checking the SNR to determine whether to quickly disconnect STAs.

The **undo smart-roam quick-kickoff-snr check-interval** command restores the default interval for checking the SNR to determine whether to quickly disconnect STAs.

The default interval for checking the SNR to determine whether to quickly disconnect STAs is 500 ms.

Format

smart-roam quick-kickoff-snr check-interval *check-interval*

undo smart-roam quick-kickoff-snr check-interval

Parameters

Parameter	Description	Value
check-interval *check-interval*	Specifies an interval for checking the SNR to determine whether to quickly disconnect STAs.	The value is an integer that ranges from 300 to 3000, in milliseconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the mode for quickly disconnecting STAs is set to **check-snr**, you can run the **smart-roam quick-kickoff-snr check-interval** command to set the interval for checking the SNR to determine whether to quickly disconnect STAs. A shorter interval allows the system to determine whether to disconnect STAs more quickly.

Prerequisites

The function of quickly disconnecting STAs has been enabled using the **undo smart-roam quick-kickoff-threshold disable** command.

Example

Set the interval for checking the SNR to determine whether to quickly disconnect STAs to 600 ms.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-snr check-interval 600
```

11.4.110 smart-roam quick-kickoff-snr p-n criteria

Function

The **smart-roam quick-kickoff-snr p-n criteria** command configures the PN threshold for quickly disconnecting STAs.

The **undo smart-roam quick-kickoff-snr p-n criteria** command restores the default PN threshold for quickly disconnecting STAs.

By default, the number of PN observation times is 6, and the number of times criteria are met is 4.

Format

smart-roam quick-kickoff-snr p-n criteria observe-time *observe-value* **qualify-time** *qualify-value*

undo smart-roam quick-kickoff-snr p-n criteria

Parameters

Parameter	Description	Value
observe-time *observe-value*	Specifies the number of PN observation times.	The value is an integer that ranges from 1 to 10.

Parameter	Description	Value
qualify-time *qualify-value*	Specifies the number of PN observation times criteria are met.	The value is an integer that ranges from 1 to 10.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the mode for quickly disconnecting STAs is set to **check-snr**, you can run the **smart-roam quick-kickoff-snr p-n criteria** command to configure the PN threshold for quickly disconnecting STAs.

PN criteria: When N conditions are met in the P range, an event is triggered. Assume that the value of **observe-value** is 6 and that of **qualify-value** is 4, and the interval for checking the SNR to determine whether to quickly disconnect STAs is 500 ms. The system detects the SNR of a STA for six consecutive times and calculates the average SNR value. If the average value is smaller than the total average value four times, the STA is forced offline.

Prerequisites

The function of quickly disconnecting STAs has been enabled using the **undo smart-roam quick-kickoff-threshold disable** command.

Precautions

The value of **observe-value** must be greater than or equal to that of **qualify-value**.

Example

Set the value of **observe-value** to 10 and that of **qualify-value** to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-snr p-n criteria observe-time 10 qualify-time 5
```


11.4.111 smart-roam quick-kickoff-threshold

Function

The **smart-roam quick-kickoff-threshold** command sets the threshold for quickly disconnecting STAs.

The **undo smart-roam quick-kickoff-threshold** command restores the default threshold for quickly disconnecting STAs.

By default, the SNR-based threshold for quickly disconnecting STAs is 15 dB, and the rate-based threshold is 20%.

Format

smart-roam quick-kickoff-threshold { **snr** *snr-threshold* | **rate** *rate-threshold* }

undo smart-roam quick-kickoff-threshold { **snr** | **rate** }

Parameters

Parameter	Description	Value
snr *snr-threshold*	Specifies the SNR-based threshold for quickly disconnecting STAs.	The value is an integer that ranges from 5 to 45, in dB. If this parameter is set to the default value, the threshold for quickly disconnecting STAs on the AirEngine 5762-16W is 10 dB.
rate *rate-threshold*	Specifies the rate-based threshold for quickly disconnecting STAs. The rate here refers to the negotiated rate based on the protocol and signal strength when a STA associates with an AP, instead of the actual rate of the STA.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of quickly disconnecting STAs is enabled and the threshold for quickly disconnecting STAs is specified for an AP using this command, the AP acquires a STA's SNR or rate from data packets sent from the STA. If the STA's SNR or rate is lower than the specified threshold, the AP forcibly disconnects the STA so that the STA can reinitiate a connection with the AP or roam to another AP with strong signals.

- A large threshold may cause STAs to go offline frequently.
- A small threshold may disable STAs from roaming to an AP with stronger signals.

This command is applicable to scenarios that have high requirements on real-time transmission, such as voice and video scenarios.

Prerequisites

The function of quickly disconnecting STAs has been enabled using the **undo smart-roam quick-kickoff-threshold disable** command.

The mode for triggering the function of quickly disconnecting STAs has been set using the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command.

Precautions

STAs may be forced to go offline through the smart roaming function or the function of quickly disconnecting STAs. If the SNR-based thresholds for the two functions are both configured, the function with a larger value is preferentially effective.

Example

Set the mode for triggering the function of quickly disconnecting STAs to **check-snr** and the threshold for quickly disconnecting STAs to 20 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold check-snr
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold snr 20
```

11.4.112 smart-roam roam-threshold { check-snr | check-rate }

Function

The **smart-roam roam-threshold { check-snr | check-rate }** command configures the trigger mode of smart roaming.

The **undo smart-roam roam-threshold** command restores the default trigger mode of smart roaming.

By default, the trigger mode of smart roaming is **check-snr**.

Format

smart-roam roam-threshold { **check-snr** | **check-rate** }*

undo smart-roam roam-threshold

Parameters

Parameter	Description	Value
check-snr	Specifies the trigger mode of smart roaming as **check SNR**.	-
check-rate	Specifies the trigger mode of smart roaming as **check rate**. The rate here refers to the negotiated rate based on the protocol and signal strength when a STA associates with an AP, instead of the actual rate of the STA.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the smart roaming function is enabled, the AP forces STAs to log out based on the configured trigger mode and threshold of smart roaming. When an AP receives a STA's data packet, the AP learns the STA's SNR or rate from the data packet. If the STA's SNR or rate is lower than the configured threshold, roaming is triggered. Then, the AP sends a Disassociation frame to the STA so that the STA can reinitiate a connection with the AP or roam to another AP with strong signals.

Prerequisites

Smart roaming or AI roaming has been enabled.

Follow-up Procedure

Run the **smart-roam roam-threshold { snr | rate }** command to configure the smart roaming threshold.

Example

Set the trigger mode of smart roaming to **check-rate**.

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



```
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] smart-roam roam-threshold check-rate
```

11.4.113 smart-roam roam-threshold { snr | rate }

Function

The **smart-roam roam-threshold { snr | rate }** command sets the smart roaming threshold.

The **undo smart-roam roam-threshold** command restores the default smart roaming threshold.

By default, the SNR threshold for smart roaming is 20 dB, and the rate threshold is 20%.

Format

smart-roam roam-threshold { **snr** *snr-threshold* | **rate** *rate-threshold* }

undo smart-roam roam-threshold { **snr** | **rate** }

Parameters

Parameter	Description	Value
snr *snr-threshold*	Specifies the SNR threshold for smart roaming. If the SNR threshold is 25 dB and noise floor is -95 dBm, a STA's SNR is lower than the threshold when the STA's RSSI is lower than -70 dBm (25 dB + (-95 dBm) = -70 dBm). **NOTE** If the signal strength of a STA is close to the smart roaming threshold, the network experience may be poor. If the default SNR threshold is used and the signal strength of many 2.4 GHz STAs is close to the smart roaming threshold, it is recommended that the 2.4 GHz and 5 GHz radios be bound to different RRM profiles and the SNR threshold be increased to about 25 dB in the RRM profile corresponding to the 2.4 GHz radio. Wait for 1 to 2 minutes and then observe the signal strength and service experience of these STAs.	The value is an integer that ranges from 15 to 45, in dB. If this parameter is set to the default value, the STA roaming threshold on the AirEngine 5762-16W is 15 dB.

Parameter	Description	Value
rate *rate-threshold*	Specifies the rate threshold for smart roaming. The rate here refers to the negotiated rate based on the protocol and signal strength when a STA associates with an AP, instead of the actual rate of the STA. If the maximum capability of the AP and STA is 54 Mbit/s and the rate threshold is 50%, the lower rate threshold is considered 27 Mbit/s (54 Mbit/s x 50% = 27 Mbit/s).	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the smart roaming function is enabled, the AP forces STAs to log out based on the configured trigger mode and threshold of smart roaming. When an AP receives a STA's data packet, the AP learns the STA's SNR or rate from the data packet. If the STA's SNR or rate is lower than the configured threshold, smart roaming is triggered. Then, the AP sends a Disassociation frame to the STA so that the STA can reinitiate a connection with the AP or roam to another AP with strong signals.

- A large threshold may cause STAs to go offline frequently.
- A small threshold may disable STAs from roaming to an AP with stronger signals.

Prerequisites

Smart roaming or AI roaming has been enabled.

The trigger mode of smart roaming has been configured using the **smart-roam roam-threshold { check-snr | check-rate }** command.

Precautions

STAs may be forced to go offline through the smart roaming function or the function of quickly disconnecting STAs. If the SNR-based thresholds for the two functions are both configured, the function with a larger value is preferentially effective.

Example

Set the trigger mode of smart roaming to **check-snr** and set the smart roaming threshold to 25 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] smart-roam roam-threshold check-snr
[HUAWEI-wlan-rrm-prof-default] smart-roam roam-threshold snr 25
```

11.4.114 smart-roam snr-margin

Function

The **smart-roam snr-margin** command sets the RSSI difference thresholds that trigger STA roaming steering.

The **undo smart-roam snr-margin** command restores the default RSSI difference thresholds that trigger STA roaming steering.

By default, the upper and lower RSSI difference thresholds that trigger STA roaming steering are 12 dB and 10 dB, respectively.

Format

smart-roam snr-margin high-level-margin *high-level-margin* **low-level-margin** *low-level-margin*

undo smart-roam snr-margin

Parameters

Parameter	Description	Value
high-level-margin *high-level-margin*	Specifies the upper RSSI difference threshold for triggering STA roaming steering.	The value is an integer that ranges from 10 to 20, in dB.
low-level-margin *low-level-margin*	Specifies the lower RSSI difference threshold for triggering STA roaming steering.	The value is an integer that ranges from 3 to 15, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In smart roaming and AI roaming scenarios, you can configure the thresholds for determining whether to steer STA roaming. When determining whether to steer a STA to roam to a neighboring AP, the AP compares the RSSIs of the STA on the neighboring AP with that on the current AP, which are reported by the STA through coordinated measurement. If the RSSI difference is higher than a specified threshold, that is, the STA has a significantly increased RSSI after associating with the neighboring AP, the AP steers the STA to roam to the neighboring AP.

The parameters **low-level-margin** and **high-level-margin** are used to determine whether to steer sticky STAs and common STAs, respectively, to roam to neighboring APs in smart roaming scenarios. In most cases, you are advised to set **high-level-margin** larger than **low-level-margin** so that sticky STAs can roam to neighboring APs with better experience as soon as possible.

In AI roaming scenarios based on coordinated measurement, only **high-level-margin** is used to determine whether to steer STAs to roam to neighboring APs.

The default difference thresholds are recommended. If APs are deployed close to each other and have high transmit power, set larger values for the upper and lower RSSI difference thresholds.

Prerequisites

Smart roaming or AI roaming has been enabled.

Example

Set the upper and lower RSSI difference thresholds that trigger STA roaming steering to 10 dB and 6 dB, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] smart-roam snr-margin high-level-margin 10 low-level-margin 6
```

11.4.115 smart-roam unable-roam-client expire-time

Function

The **smart-roam unable-roam-client expire-time** command sets the aging time of the "unable to roam" record for STAs.

The **undo smart-roam unable-roam-client expire-time** command restores the default aging time of the "unable to roam" record for STAs.

By default, the aging time of an "unable to roam" record is 30 minutes.

Format

smart-roam unable-roam-client expire-time *expire-time*

undo smart-roam unable-roam-client expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time of the "unable to roam" record.	The value is an integer that ranges from 30 to 2880, in minutes.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After smart roaming is enabled, you can run the **smart-roam unable-roam-client expire-time** command to set the aging time of the "unable to roam" record for STAs. When the device requests a STA to roam but the STA keeps sending association requests to the original AP or does not initiate an association request, the device records the terminal as "unable to roam" and does not trigger STA roaming within the specified time. After the aging time is reached, the "unable to roam" record for STAs is automatically cleared, and the system can trigger roaming of the STAs.

A STA is recorded as "unable to roam" due to the following reasons:

- Due to different software configurations, some STAs preferentially send association requests to APs with which they have once associated.
- In some environments, STAs cannot scan APs with strong signals.
- STAs enter the dormancy state and do not roam once they are forcibly disconnected.

The aging time to configure varies for different reasons. A large aging time is used for the software configuration reason so that the AP will trigger roaming of the STAs as less as possible. However, a small aging time is used in other situations so that the AP will attempt to trigger roaming of the STAs marked "unable to roam."

Prerequisites

Smart roaming or AI roaming has been enabled.

Example

Set the aging time of the "unable to roam" record to 50 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
```



```
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] smart-roam unable-roam-client expire-time 50
```

11.4.116 spatial-reuse disable

Function

The **spatial-reuse disable** command disables the spatial reuse (SR) function.

The **undo spatial-reuse disable** command enables the SR function.

By default, the SR function is enabled.

NOTE

The SR function is not supported by the following APs:

- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762

Format

spatial-reuse disable

undo spatial-reuse disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

The BSS coloring function has been enabled.

Precautions

Disabling the BSS coloring function will automatically disable the spatial reuse (SR) function.

Example

Disable the SR function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] spatial-reuse disable
```


11.4.117 sta-load-balance dynamic btm-fail-times

Function

The **sta-load-balance dynamic btm-fail-times** command sets the maximum number of attempts to steer STAs in BTM mode.

The **undo sta-load-balance dynamic btm-fail-times** command restores the default maximum number of attempts to steer STAs in BTM mode.

By default, the maximum number of attempts to steer STAs in BTM mode is 5.

Format

sta-load-balance dynamic btm-fail-times *btm-fail-times*

undo sta-load-balance dynamic btm-fail-times

Parameters

Parameter	Description	Value
btm-fail-times	Specifies the maximum number of attempts to steer STAs in BTM mode.	The value is an integer that ranges from 0 to 10. The value 0 indicates that the BTM mode is not used to steer STAs.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device preferentially uses the BTM mode to trigger STA steering to the target AP. Due to differences of STAs, some STAs can be successfully steered in BTM mode after multiple attempts. You can run the **sta-load-balance dynamic btm-fail-times** command to set the maximum number of attempts to steer STAs in BTM mode. If the number of attempts exceeds the specified value, the device attempts to steer STAs in deauthentication mode.

Precautions

You are advised to retain the default value. If the success rate of STA steering in BTM mode is low, you can set a smaller value to improve the steering efficiency.

Example

Set the maximum number of attempts to steer STAs in BTM mode to 4 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic btm-fail-times 4
```

11.4.118 sta-load-balance dynamic deauth-fail-times

Function

The **sta-load-balance dynamic deauth-fail-times** command sets the maximum number of attempts to steer STAs in deauthentication mode.

The **undo sta-load-balance dynamic deauth-fail-times** command restores the default maximum number of attempts to steer STAs in deauthentication mode.

By default, the maximum number of attempts to steer STAs in deauthentication mode is 0.

Format

sta-load-balance dynamic deauth-fail-times *deauth-fail-times*

undo sta-load-balance dynamic deauth-fail-times

Parameters

Parameter	Description	Value
deauth-fail-times	Specifies the maximum number of attempts to steer STAs in deauthentication mode.	The value is an integer that ranges from 0 to 5. The value 0 indicates that the deauthentication mode is not used to steer STAs.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device attempts to use the 802.11v and deauthentication modes to trigger STA steering to the target AP. Due to differences of STAs, some STAs can be successfully steered in deauthentication mode after multiple attempts. You can run the **sta-load-balance dynamic deauth-fail-times** command to set the maximum number of attempts to steer STAs in deauthentication mode. If the number of attempts exceeds the specified value, STAs cannot be steered.

Precautions

You are advised to retain the default value. If the success rate of STA steering in deauthentication mode is low or STA services are affected, set the parameter value to 0 to disable STA steering in deauthentication mode.

Example

Set the maximum number of attempts to steer STAs in deauthentication mode to 1 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic deauth-fail-times 1
```

11.4.119 sta-load-balance dynamic disable

Function

The **sta-load-balance dynamic disable** command disables the dynamic load balancing function.

The **undo sta-load-balance dynamic disable** command enables the dynamic load balancing function.

By default, the dynamic load balancing function is enabled.

Format

sta-load-balance dynamic disable

undo sta-load-balance dynamic disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Static load balancing limits the maximum number of AP radios to 16 and allows only radios on the same frequency band to join a load balancing group.

Additionally, a load balancing group needs to be manually specified. Dynamic load balancing overcomes the limitations of static load balancing.

After a STA connects to an AP, the AC checks whether the AP reaches the load balancing threshold, and determines whether to steer the STA to a neighboring AP that meets load balancing requirements based on the load balancing algorithm.

Example

Disable dynamic load balancing.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic disable
```

11.4.120 sta-load-balance dynamic sta-number gap-threshold

Function

The **sta-load-balance dynamic sta-number gap-threshold** command sets the load difference threshold for dynamic load balancing based on the number of users.

The **undo sta-load-balance dynamic sta-number gap-threshold** command restores the default load difference threshold for dynamic load balancing based on the number of users.

By default, the load difference threshold of a dynamic load balancing group is specified based on the number of users, and the default value is 3.

Format

sta-load-balance dynamic sta-number gap-threshold { **percentage** *percentage-value* | **number** *number-value* }

undo sta-load-balance dynamic sta-number gap-threshold

Parameters

Parameter	Description	Value
percentage *percentage-value*	Specifies the load difference threshold for dynamic load balancing based on the percentage of users.	The value is an integer that ranges from 1 to 100. It indicates the threshold of the load difference among radios in a load balancing group, in percentage. The load difference refers to the difference between the percentages of users on radios.

Parameter	Description	Value
number *number-value*	Specifies the load difference threshold for dynamic load balancing based on the number of users.	The value is an integer that ranges from 1 to 20. It indicates the threshold of the load difference among radios in a load balancing group. The load difference refers to the difference between the numbers of users on radios.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user requests to connect to an AP, the AP counts the total number of access users on all radios. If the total number of access users does not exceed the start threshold configured using the **sta-load-balance dynamic sta-number start-threshold** command, the AP does not implement dynamic load balancing. The AP implements dynamic load balancing only when the total number of access users on all radios exceeds the start threshold.

The following load balancing algorithm is used after the user access to determine whether to steer the user to a new AP:

One of the conditions for steering a user to a new AP is that the radio of the target load is lower than that of the current access radio. The radio load is identified by the number or percentage (Number of users associated with the current radio/Maximum number of access users supported by the radio x 100%) of access users. If the load difference between the target radio and current radio exceeds the specified threshold, the condition is met.

NOTE

The start threshold and load difference threshold for dynamic load balancing are used to adjust the sensitivity for triggering load balancing, and the default values are recommended. If the start and load difference thresholds are set low, load balancing becomes far easier to be triggered. As a result, STAs are frequently switched between APs, affecting user experience. If the start and load difference thresholds are set high, the load balancing mechanism may become invalid.

Precautions

If you configure the load difference threshold based on both the number of users and the percentage of users, only the latest configuration takes effect.

Example

Set the load difference threshold for dynamic load balancing based on the number of users to 25% in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic sta-number gap-threshold percentage 25
```

11.4.121 sta-load-balance dynamic sta-number start-threshold

Function

The **sta-load-balance dynamic sta-number start-threshold** command sets the start threshold for dynamic load balancing based on the number of users.

The **undo sta-load-balance dynamic sta-number start-threshold** command restores the default start threshold for dynamic load balancing based on the number of users.

By default, the start threshold for dynamic load balancing based on the number of users is 10.

Format

sta-load-balance dynamic sta-number start-threshold *start-threshold*

undo sta-load-balance dynamic sta-number start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold*	Specifies the start threshold for dynamic load balancing based on the number of users.	The value is an integer that ranges from 1 to 40.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When a user requests to connect to an AP, the AP counts the total number of access users on all radios. If the number of access users on the requested radio does not exceed the start threshold, the AP does not implement dynamic load

balancing based on the number of users. The AP implements dynamic load balancing based on the number of users only after the number of access users exceeds the start threshold.

NOTE

The start and load difference thresholds for dynamic load balancing configured using the **sta-load-balance dynamic sta-number gap-threshold** command can be used to adjust sensitivity for triggering load balancing. The default values are recommended in typical scenarios. A higher threshold is recommended in high-density scenarios. If the start and load difference thresholds are set low, load balancing becomes far easier to be triggered. As a result, STAs are frequently switched between APs, affecting user experience. If the start and load difference thresholds are set high, the load balancing mechanism may become invalid.

Example

Set the start threshold for dynamic load balancing based on the number of users to 20 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic sta-number start-threshold 20
```

11.4.122 sta-load-balance static-group

Function

The **sta-load-balance static-group** command creates a static load balancing group and displays the static load balancing group view.

The **undo sta-load-balance static-group** command deletes a static load balancing group.

By default, no static load balancing group is configured.

Format

sta-load-balance static-group name *group-name*

undo sta-load-balance static-group { **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a load balancing group.	The value is a string of 1 to 35 plaintext characters. It does not contain any question mark (?) and cannot begin or end with double quotation marks (" ").
all	Deletes all static load balancing groups.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

In static load balancing mode, APs providing the same services are manually added to a load balancing group. When a STA needs to access a WLAN, it sends an Association Request packet to an AC through an AP. The AC determines whether to allow access from the STA according to the load balancing algorithm.

To configure static load balancing, run the **sta-load-balance static-group** command in the WLAN view to create a static load balancing group and **member (static load balancing group view)** command to add APs to the group.

Example

Configure the static load balancing group named **new**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name new
[HUAWEI-wlan-sta-lb-static-new]
```

11.4.123 sta-number start-threshold

Function

The **sta-number start-threshold** command sets the start threshold for load balancing based on the number of users in a static load balancing group.

The **undo sta-number start-threshold** command deletes the configured start threshold for load balancing based on the number of users in a static load balancing group.

By default, the start threshold for load balancing based on the number of users in a static load balancing group is 10.

Format

sta-number start-threshold *start-threshold-value*

undo sta-number start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold-value*	Specifies the start threshold for load balancing based on the number of users in a static load balancing group.	The value is an integer that ranges from 1 to 40.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to set the start threshold for load balancing based on the number of users in a static load balancing group. If the load on a radio does not reach the start threshold, the device does not implement load balancing control on access STAs.

Example

Set the start threshold for load balancing based on the number of users in the static load balancing group to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] sta-number start-threshold 5
```

11.4.124 sta-load-balance dynamic probe-report interval

Function

The **sta-load-balance dynamic probe-report interval** command sets the interval for reporting Probe frames.

The **undo sta-load-balance dynamic probe-report interval** command restores the default interval for reporting Probe frames.

By default, Probe frames are reported at an interval of 120 seconds.

Format

sta-load-balance dynamic probe-report interval *interval*

undo sta-load-balance dynamic probe-report interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for reporting Probe frames.	The value is an integer that ranges from 30 to 300, in seconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP collects information about neighboring APs of STAs and reports the information to the AC for determining the target APs to which the STAs will roam. You can run this command to set the interval at which an AP reports information about neighboring APs of STAs.

Precautions

You are advised to retain the default value. If the device has high performance pressure, you can set a longer interval.

Example

Set the interval for reporting Probe frames to 125 seconds in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic probe-report interval 125
```

11.4.125 sta-load-balance dynamic rssi-diff-gap

Function

The **sta-load-balance dynamic rssi-diff-gap** command sets the RSSI difference threshold for members in a dynamic load balancing group.

The **undo sta-load-balance dynamic rssi-diff-gap** command restores the default RSSI difference threshold of members in a dynamic load balancing group.

By default, the RSSI difference threshold of members in a dynamic load balancing group is 5 dB.

Format

sta-load-balance dynamic rssi-diff-gap *diff-gap-threshold*

undo sta-load-balance dynamic rssi-diff-gap

Parameters

Parameter	Description	Value
diff-gap-threshold	Specifies the RSSI difference threshold of members in a dynamic load balancing group.	The value is an integer that ranges from 0 to 15, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To achieve load balancing, an AP may steer connected STAs to other APs with smaller RSSIs. If the RSSI of the AP with which a STA currently associates minus the RSSI of the target AP is larger than the specified RSSI difference threshold, the STA is denied from being steered to the target AP; otherwise, the STA can be steered to the target AP.

Precautions

If STAs have high signal quality deterioration tolerance for the target AP, you can set a larger RSSI difference threshold to achieve better load balancing effect. If STAs have low signal quality deterioration tolerance for the target AP, set a smaller RSSI difference threshold. You are advised to retain the default value.

Example

Set the RSSI difference threshold of members in a dynamic load balancing group to 6 dB in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic rssi-diff-gap 6
```


11.4.126 sta-load-balance dynamic rssi-threshold

Function

The **sta-load-balance dynamic rssi-threshold** command sets an RSSI threshold for member devices in a dynamic load balancing group.

The **undo sta-load-balance dynamic rssi-threshold** command restores the default RSSI threshold of member devices in a dynamic load balancing group.

By default, the RSSI threshold of member devices in a dynamic load balancing group is –65 dBm.

Format

sta-load-balance dynamic rssi-threshold *rssi-threshold*

undo sta-load-balance dynamic rssi-threshold

Parameters

Parameter	Description	Value
rssi-threshold	Specifies the RSSI threshold of member devices in a dynamic load balancing group.	The value is an integer that ranges from –75 to –55, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the RSSI threshold of member devices in a dynamic load balancing group is configured, an AP compares the RSSI of a STA with the configured RSSI threshold after receiving the Probe Request packet sent by the STA. If the STA's RSSI exceeds the threshold, the AP reports STA information to the AC, and the AP is added to the dynamic load balancing group. If the STA's RSSI does not exceed the threshold, the AP directly filters STA information and does not report the information to the AC, and the AP is not added to the dynamic load balancing group.

Setting an RSSI threshold for member devices in a dynamic load balancing group is to filter APs with weak signals, so that STAs can be load-balanced between APs with better signals. This prevents STAs from associating with APs with weak signals but light loads. This function does not affect STAs' going online.

Example

Set the RSSI threshold for member devices in a dynamic load balancing group to –70 dBm in the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic rssi-threshold -70
```

11.4.127 sta-load-balance dynamic steer-restrict auth-threshold

Function

The **sta-load-balance dynamic steer-restrict auth-threshold** command sets the maximum number of times non-target APs suppress authentication of STAs during STA steering.

The **undo sta-load-balance dynamic steer-restrict auth-threshold** command restores the default maximum number of times non-target APs suppress authentication of STAs during STA steering.

By default, the maximum number of times non-target APs suppress authentication of STAs during STA steering is 0.

Format

sta-load-balance dynamic steer-restrict auth-threshold *auth-threshold*

undo sta-load-balance dynamic steer-restrict auth-threshold

Parameters

Parameter	Description	Value
auth-threshold	Specifies the maximum number of times non-target APs suppress authentication of STAs during STA steering.	The value is an integer that ranges from 0 to 5.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success

rate. You can run the **sta-load-balance dynamic steer-restrict auth-threshold** command to set the maximum number of times non-target APs suppress authentication of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the maximum number of times non-target APs suppress authentication of STAs during STA steering to 1 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic steer-restrict auth-threshold 1
```

11.4.128 sta-load-balance dynamic steer-restrict probe-threshold

Function

The **sta-load-balance dynamic steer-restrict probe-threshold** command sets the maximum number of times non-target APs suppress probing of STAs during STA steering.

The **undo sta-load-balance dynamic steer-restrict probe-threshold** command restores the default maximum number of times non-target APs suppress probing of STAs during STA steering.

By default, the maximum number of times non-target APs suppress probing of STAs during STA steering is 5.

Format

sta-load-balance dynamic steer-restrict probe-threshold *probe-threshold*

undo sta-load-balance dynamic steer-restrict probe-threshold

Parameters

Parameter	Description	Value
probe-threshold	Specifies the maximum number of times non-target APs suppress probing of STAs during STA steering.	The value is an integer that ranges from 0 to 10.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict probe-threshold** command to set the maximum number of times non-target APs suppress probing of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the maximum number of times non-target APs suppress probing of STAs during STA steering to 4 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic steer-restrict probe-threshold 4
```

11.4.129 sta-load-balance dynamic steer-restrict restrict-time

Function

The **sta-load-balance dynamic steer-restrict restrict-time** command sets the duration within which non-target APs suppress association of STAs during STA steering.

The **undo sta-load-balance dynamic steer-restrict restrict-time** command restores the default duration within which non-target APs suppress association of STAs during STA steering.

By default, the duration within which non-target APs suppress association of STAs during STA steering is 5 seconds.

Format

sta-load-balance dynamic steer-restrict restrict-time *restrict-time*

undo sta-load-balance dynamic steer-restrict restrict-time

Parameters

Parameter	Description	Value
restrict-time	Specifies the duration within which non-target APs suppress association of STAs during STA steering.	The value is an integer that ranges from 0 to 10, in seconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict restrict-time** command to set the duration within which non-target APs suppress association of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the duration within which non-target APs suppress association of STAs during STA steering to 4 seconds in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic steer-restrict restrict-time 4
```

11.4.130 sta-profiling disable

Function

The **sta-profiling disable** command disables the STA profiling function.

The **undo sta-profiling disable** command enables the STA profiling function.

By default, the STA profiling function is enabled.

Format

sta-profiling disable

undo sta-profiling disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

On a traditional WLAN, when a STA is far away from an AP, the signal strength of the STA gradually weakens and the Internet access rate of the STA becomes lower and lower. If the STA is always associated with an existing AP, user experience deteriorates. With the smart roaming mechanism, the system can automatically steer STAs encountered with poor network quality to APs providing better signals. In practice, the roaming process depends on multiple negotiations between APs and STAs. STAs of different vendors and models have different autonomous behaviors during the negotiation process. As a result, roaming experience cannot be effectively guaranteed. After the STA profiling function is enabled, the system can create profiles for STAs of this type based on the STA behaviors and learn how to steer roaming for these STAs more effectively. This improves the roaming sensitivity and success rate, enhancing the roaming experience of users.

Example

Disable the STA profiling function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-profiling disable
```

11.4.131 steer-restrict auth-threshold

Function

The **steer-restrict auth-threshold** command sets the maximum number of times non-target APs suppress authentication of STAs during STA steering.

The **undo steer-restrict auth-threshold** command restores the default maximum number of times non-target APs suppress authentication of STAs during STA steering.

By default, the maximum number of times non-target APs suppress authentication of STAs during STA steering is 0.

Format

steer-restrict auth-threshold *auth-threshold*

undo steer-restrict auth-threshold

Parameters

Parameter	Description	Value
auth-threshold	Specifies the maximum number of times non-target APs suppress authentication of STAs during STA steering.	The value is an integer that ranges from 0 to 5.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict auth-threshold** command to set the maximum number of times non-target APs suppress authentication of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the maximum number of times non-target APs suppress authentication of STAs during STA steering to 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] steer-restrict auth-threshold 1
```


11.4.132 steer-restrict probe-threshold

Function

The **steer-restrict probe-threshold** command sets the maximum number of times non-target APs suppress probing of STAs during STA steering.

The **undo steer-restrict probe-threshold** command restores the default maximum number of times non-target APs suppress probing of STAs during STA steering.

By default, the maximum number of times non-target APs suppress probing of STAs during STA steering is 5.

Format

steer-restrict probe-threshold *probe-threshold*

undo steer-restrict probe-threshold

Parameters

Parameter	Description	Value
probe-threshold	Specifies the maximum number of times non-target APs suppress probing of STAs during STA steering.	The value is an integer that ranges from 0 to 10.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict probe-threshold** command to set the maximum number of times non-target APs suppress probing of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the maximum number of times non-target APs suppress probing of STAs during STA steering to 4.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] steer-restrict probe-threshold 4
```

11.4.133 steer-restrict restrict-time

Function

The **steer-restrict restrict-time** command sets the duration within which non-target APs suppress association of STAs during STA steering.

The **undo steer-restrict restrict-time** command restores the default duration within which non-target APs suppress association of STAs during STA steering.

By default, the duration within which non-target APs suppress association of STAs during STA steering is 5 seconds.

Format

steer-restrict restrict-time *restrict-time*

undo steer-restrict restrict-time

Parameters

Parameter	Description	Value
restrict-time	Specifies the duration within which non-target APs suppress association of STAs during STA steering.	The value is an integer that ranges from 0 to 10, in seconds.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict restrict-time**

command to set the duration within which non-target APs suppress association of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the duration within which non-target APs suppress association of STAs during STA steering to 4 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] steer-restrict restrict-time 4
```

11.4.134 terminal-identify disable

Function

The **terminal-identify disable** command disables the terminal identification 2.0 function on an AP.

The **undo terminal-identify disable** command enables the terminal identification 2.0 function on an AP.

By default, the terminal identification 2.0 function is enabled on an AP.

Format

terminal-identify disable

undo terminal-identify disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

After a terminal accesses an AP enabled with the terminal identification 2.0 function, the system extracts terminal type information from the DHCP, mDNS, and HTTP packets from the terminal to identify the terminal type.

NOTE

The AI roaming and terminal identification 2.0 functions are not supported by the following APs:

- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762
- AirEngine 9700D series central APs (including matching RUs)
- AirEngine 9700D-S (including matching ORUs)

Example

Enable the terminal identification 2.0 function on the target AP in the AP system profile **ap-system1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] undo terminal-identify disable
```

11.4.135 uac enable

Function

The **uac enable** command enables user CAC.

The **undo uac enable** command disables user CAC.

By default, user CAC is disabled.

Format

uac { **client-number** | **client-snr** } **enable**

undo uac { **client-number** | **client-snr** } **enable**

Parameters

Parameter	Description	Value
client-number	Controls user access based on the number of users.	-
client-snr	Controls user access based on the terminal SNR.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On WLANs where many users exist, such as WLANs in high density scenarios, users compete fiercely to occupy resources as the number of online users increases. As a result, network quality deteriorates. To ensure network access experience of online users, configure the user CAC function. The user CAC function allows an AP to control user access based on the number of online users or terminal SNR, which enables provisioning of high-quality network access services.

CAC is implemented in the following modes:

- User CAC based on the number of users uses a simple algorithm. This mode is recommended when most users have the same type of services and similar service traffic volumes.
- SNR-based user CAC controls access from weak-signal users, and is applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

CAC based on the number of users can be configured together with SNR-based CAC.

Follow-up Procedure

Run the **uac client-number threshold** command to set the user CAC threshold based on the number of users.

Run the **uac client-snr threshold** command to set the user CAC threshold based on terminal SNR.

Run the **uac reach-access-threshold** { **hide-ssid** | **priority-replace** } command to configure the action to take for subsequent access control when the number of access users reaches the user CAC threshold.

Example

Enable user CAC based on the number of users.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] uac client-number enable
```

11.4.136 uac client-number threshold

Function

The **uac client-number threshold** command configures the user CAC threshold based on the number of users.

The **undo uac client-number threshold** command restores the default user CAC threshold based on the number of users.

By default, the user CAC access and roaming thresholds based on the number of users are both 64.

Format

uac client-number threshold access *access-threshold* [**roam** *roam-threshold*]

undo uac client-number threshold

Parameters

Parameter	Description	Value
access *access-threshold*	Specifies the user CAC access threshold based on the number of users.	The value is an integer that ranges from 1 to 512.
roam *roam-threshold*	Specifies the user CAC roaming threshold based on the number of users. This threshold is the total number of users who can be associate with the AP, including all local and reassociated roaming users.	The value is an integer that ranges from 1 to 512.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On WLANs where many users exist, such as WLANs in high density scenarios, users compete fiercely to occupy resources as the number of online users increases. As a result, network quality deteriorates. To ensure network access experience of online users, configure the user CAC function. The user CAC function allows an AP to control user access based on the number of online users or terminal SNR, which enables provisioning of high-quality network access services.

NOTE

The user CAC access threshold is invalid for roaming users. For example, the user CAC access threshold is 20, and the user CAC roaming threshold is 24. If 20 local users have already connected to the network, not more local users can connect to the network but another four roaming users can.

CAC is implemented in the following modes:

- User CAC based on the number of users uses a simple algorithm. This mode is recommended when most users have the same type of services and similar service traffic volumes.

- SNR-based user CAC controls access from weak-signal users, and is applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

CAC based on the number of users can be configured together with SNR-based CAC.

Prerequisites

The user CAC function based on the number of users has been enabled using the **uac client-number enable** command.

Example

Set the user CAC access threshold based on the number of users to 50 and the roaming threshold to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] uac client-number enable
[HUAWEI-wlan-rrm-prof-test] uac client-number threshold access 50 roam 60
```

11.4.137 uac client-snr threshold

Function

The **uac client-snr threshold** command configures the user CAC threshold based on terminal SNR.

The **undo uac client-snr threshold** command restores the default user CAC threshold based on terminal SNR.

By default, the user CAC threshold based on terminal SNR is 15 dB.

Format

uac client-snr threshold *threshold*

undo uac client-snr threshold

Parameters

Parameter	Description	Value
threshold	Specifies the user CAC threshold based on terminal SNR.	The value is an integer that ranges from 5 to 45, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On WLANs where many users exist, such as WLANs in high density scenarios, users compete fiercely to occupy resources as the number of online users increases. As a result, network quality deteriorates. To ensure network access experience of online users, configure the user CAC function. The user CAC function allows an AP to control user access based on the number of online users or terminal SNR, which enables provisioning of high-quality network access services.

The configured user CAC threshold based on terminal SNR takes effect for new STAs. When a new STA (or a roaming STA) attempts to connect to an AP, the AP checks the STA's SNR. If the SNR is smaller than the threshold, the AP denies the STA's access.

CAC is implemented in the following modes:

- User CAC based on the number of users uses a simple algorithm. This mode is recommended when most users have the same type of services and similar service traffic volumes.
- SNR-based user CAC controls access from weak-signal users, and is applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

CAC based on the number of users can be configured together with SNR-based CAC.

Prerequisites

The user CAC function based on terminal SNR has been enabled using the **uac client-snr enable** command.

Example

Set the user CAC threshold based on terminal SNR to 16 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] uac client-snr enable
[HUAWEI-wlan-rrm-prof-default] uac client-snr threshold 16
```

11.4.138 uac reach-access-threshold

Function

The **uac reach-access-threshold** command configures the user CAC function and specifies the action to take when the number of access users reaches the user CAC threshold.

The **undo uac reach-access-threshold** command disables SSID hiding or priority-based user replacement.

By default, SSID hiding and priority-based user replacement are disabled.

Format

uac reach-access-threshold { **hide-ssid** | **priority-replace** }

undo uac reach-access-threshold

Parameters

Parameter	Description	Value
hide-ssid	Indicates SSID hiding.	-
priority-replace	Indicates priority-based user replacement.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After user CAC is configured, you can configure the action to take when the number of access users reaches the threshold. The following actions are available:

- Deny new user access. This is the default configuration.
- Deny new user access and hide the SSID.
- Disconnect common users to make room for access of high-priority users.

Prerequisites

User CAC has been enabled using the **uac** { **client-number** | **client-snr** } **enable** command.

Precautions

- When you run the **undo uac** { **client-number** | **client-snr** } **enable** command to disable user CAC, SSID hiding is automatically canceled.
- The **uac reach-access-threshold priority-replace** command takes effect only when UAC based on the number of users is enabled.

Example

Enable SSID hiding.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] uac client-number enable
[HUAWEI-wlan-rrm-prof-test] uac reach-access-threshold hide-ssid
```

Enable priority-based user replacement.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] uac client-number enable
[HUAWEI-wlan-rrm-prof-test] uac reach-access-threshold priority-replace
Info: This configuration only takes effective when uac client-number enabled.
```

Deny new user access.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] undo uac reach-access-threshold
```

11.5 WLAN Spectrum Analysis Configuration Commands

11.5.1 Command Support

- WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.
- Starting from V200R020C10, AirEngine X760 series APs support spectrum analysis. To implement spectrum analysis on the following APs, upgrade them to V200R020C10 or later: AirEngine 8760-X1-PRO, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD. If the AC version is earlier than V200R020C10, run the **undo ap-type** command on the AC to delete the AP type, which will cause corresponding APs to go offline. Then manually add the AP type again. Alternatively, upgrade the AC to V200R020C10 or later.
- Spectrum analysis is not supported by the following APs:
  - AirEngine 8771-X1T
  - AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
  - AirEngine X762

11.5.2 channel-monitor enable

Function

The **channel-monitor enable** command enables the function of monitoring the status of all channels.

The **undo channel-monitor enable** command disables the function of monitoring the status of all channels.

By default, the function of monitoring the status of all channels is disabled.

Format

channel-monitor enable

undo channel-monitor enable

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During spectrum analysis, APs report air scan results to a spectrum server. Then the spectrum server analyzes interference source types and identifies non-Wi-Fi interference devices. After you run the **channel-monitor enable** command, APs can scan the status of all channels (normally occupied, Wi-Fi interference, non-Wi-Fi interference, or idle) over the air interface to identify all interference sources.

Precautions

To identify non-Wi-Fi interference, you also need to enable spectrum analysis.

Channels to be monitored are the same as those in the air scan channel set. To collect as much interference source information as possible within the range allowed by local laws and regulations, you are advised to run the **scan-channel-set country-channel** command to add all channels supported by the country code to the air scan channel set.

Follow-up Procedure

To display and analyze monitoring results on iMaster NCE-CampusInsight, configure interconnection with iMaster NCE-CampusInsight through the WMI mechanism and run the **collect-item radio-data** command to enable the function of reporting radio monitoring data to iMaster NCE-CampusInsight.

Example

Enable the function of monitoring the status of all channels.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] channel-monitor enable
```

11.5.3 display spectrum-analysis server-reporter

Function

The **display spectrum-analysis server-reporter** command displays a list of APs that report spectrum packets to the spectrum server.

Format

display spectrum-analysis server-reporter

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display spectrum-analysis server-reporter** command displays a list of APs that report spectrum packets to the spectrum server.

Example

Display all APs that report spectrum packets to the spectrum server.

```
<HUAWEI> display spectrum-analysis server-reporter
-------------------------------------------------------------
ID    AP name                       Radio ID
-------------------------------------------------------------
1     AP_1                          0
-------------------------------------------------------------
Total: 1
```

Table 11-157 Description of the **display spectrum-analysis server-reporter** command output

Item	Description
ID	ID of the AP that reports spectrum data. To configure this parameter, run the **spectrum-report** command.
AP name	Name of the AP that reports spectrum data. To configure this parameter, run the **spectrum-report** command.
Radio ID	ID of the radio on which the function of reporting spectrum data is enabled. To configure this parameter, run the **spectrum-report** command.

11.5.4 display wlan non-wifi-device

Function

The **display wlan non-wifi-device** command displays information about detected non-Wi-Fi devices.

Format

display wlan non-wifi-device { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Displays information about the non-Wi-Fi devices detected by all APs.	-
ap-name *ap-name*	Displays information about the non-Wi-Fi devices detected by a specified AP name.	The AP name must exist.
ap-id *ap-id*	Displays information about the non-Wi-Fi devices detected by a specified AP ID.	The AP ID must exist.
radio *radio-id*	Displays information about the non-Wi-Fi devices detected by a specified AP radio.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: • AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 • AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T • AirEngine 8771-X1T

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the function of reporting spectrum data is enabled on an AP radio using the **spectrum-report** command, you can run the **display wlan non-wifi-device** command to check information about the detected non-Wi-Fi devices.

Example

Display information about the non-Wi-Fi devices detected by all APs.

```
<HUAWEI> display wlan non-wifi-device all
Info: This operation may take a few seconds. Please wait for a moment.done.
------------------------------------------------------------------
Detect AP ID                          : 11
Detect AP name                        : 00e0-fc00-0011
Detect AP radio ID                    : 0
Detect AP channel                     : 1
Non-Wi-Fi device type                 : 4
Non-Wi-Fi device name                 : Bluetooth
Non-Wi-Fi device frequency type       : hop Frequency
Non-Wi-Fi device channel              : 7,11
Non-Wi-Fi device RSSI                 : -54,-53
Non-Wi-Fi device detect time last     : 2021-04-22/09:46:23
Non-Wi-Fi device center frequency(MHz) : 2443
Non-Wi-Fi device bandwidth(KHz)       : 3281
Non-Wi-Fi device duty(%)              : 66
Non-Wi-Fi device interfere level      : 3
------------------------------------------------------------------
------------------------------------------------------------------
Detect AP ID                          : 11
Detect AP name                        : 00e0-fc00-0010
Detect AP radio ID                    : 0
Detect AP channel                     : 1
Non-Wi-Fi device type                 : 8
Non-Wi-Fi device name                 : Babymonitor
Non-Wi-Fi device frequency type       : hop Frequency
Non-Wi-Fi device channel              : 7,13
Non-Wi-Fi device RSSI                 : -35,-48
Non-Wi-Fi device detect time last     : 2021-04-22/09:46:34
Non-Wi-Fi device center frequency(MHz) : 2443
Non-Wi-Fi device bandwidth(KHz)       : 10937
Non-Wi-Fi device duty(%)              : 39
Non-Wi-Fi device interfere level      : 3
------------------------------------------------------------------
Total: 2
```

Table 11-158 Description of the **display wlan non-wifi-device** command output

Item	Description
Detect AP ID	ID of the AP that has detected a non-Wi-Fi device.
Detect AP name	Name of the AP that has detected a non-Wi-Fi device.
Detect AP radio ID	ID of the AP radio on which a non-Wi-Fi device is detected.

Item	Description
Detect AP channel	ID of the AP channel on which a non-Wi-Fi device is detected.
Non-Wi-Fi device type	Type of the detected non-Wi-Fi device. • 0: Cordless phone • 1: Cordless phone base • 2: ZigBee device • 3: Microwave oven • 4: Bluetooth • 5: Game controller • 6: 2.4G wireless video and audio device • 7: 5G wireless video and audio device • 8: Baby monitor • 9: Fixed-frequency device
Non-Wi-Fi device name	Name of the non-Wi-Fi device.
Non-Wi-Fi device frequency type	Frequency type of the non-Wi-Fi device.
Non-Wi-Fi device channel	Channel of the non-Wi-Fi device.
Non-Wi-Fi device RSSI	RSSI of the non-Wi-Fi device.
Non-Wi-Fi device detect time last	Detection time for the non-Wi-Fi device.
Non-Wi-Fi device center frequency(MHz)	Center frequency of the non-Wi-Fi device.
Non-Wi-Fi device bandwidth(KHz)	Bandwidth of the non-Wi-Fi device.
Non-Wi-Fi device duty(%)	Duty cycle of the non-Wi-Fi device.
Non-Wi-Fi device interfere level	Interference level of the non-Wi-Fi device. The value ranges from 0 to 3. A larger value indicates stronger interference.

11.5.5 display wlan non-wifi-device history

Function

The **display wlan non-wifi-device history** command displays information about non-Wi-Fi devices in the historical list.

Format

display wlan non-wifi-device history { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Displays information about all the non-Wi-Fi devices in the historical list.	-
ap-name *ap-name*	Displays information about the non-Wi-Fi devices detected by an AP with a specified name in the historical list.	The AP name must exist.
ap-id *ap-id*	Displays information about the non-Wi-Fi devices detected by an AP with a specified ID in the historical list.	The AP ID must exist.
radio *radio-id*	Displays information about the non-Wi-Fi devices detected by a specified AP radio in the historical list.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: • AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 • AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T • AirEngine 8771-X1T

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If information about a non-Wi-Fi device is not detected within the aging time configured using the **spectrum-analysis non-wifi-device aging-time** command, the AC adds the device to the historical list.

Example

Display information about non-Wi-Fi devices in the historical list.

```
<HUAWEI> display wlan non-wifi-device history all
------------------------------------------------------------------------
S/No.                                : 0
Detect AP name                       : MyAP
Detect AP radio ID                   : 1
Detect AP channel                    : 44
Non-Wi-Fi device type                : 9
Non-Wi-Fi device name                : Unknown fix freq device
Non-Wi-Fi device frequency type      : Narrow bandwidth
Non-Wi-Fi device channel             : 147,148
Non-Wi-Fi device RSSI                : -59,-66
Non-Wi-Fi device detect time last    : 2014-11-19/17:05:05
Non-Wi-Fi device center frequency(MHz) : 5739
Non-Wi-Fi device bandwidth(KHz)      : 2708
Non-Wi-Fi device duty(%)             : 79
Non-Wi-Fi device interfere level     : 3
------------------------------------------------------------------------
Total: 1
```

Table 11-159 Description of the **display wlan non-wifi-device history** command output

Item	Description
S/No.	No.of historical records.
Detect AP name	Name of the AP that has detected a non-Wi-Fi device.
Detect AP radio ID	ID of the AP radio on which a non-Wi-Fi device is detected.
Detect AP channel	AP channel on which a non-Wi-Fi device is detected.
Non-Wi-Fi device type	Type of the detected non-Wi-Fi device.
Non-Wi-Fi device name	Name of the non-Wi-Fi device.
Non-Wi-Fi device frequency type	Frequency type of the non-Wi-Fi device.
Non-Wi-Fi device RSSI	RSSI of the non-Wi-Fi device.
Non-Wi-Fi device channel	Channel of the non-Wi-Fi device.
Non-Wi-Fi device detect time last	Detection time for the non-Wi-Fi device.
Non-Wi-Fi device center frequency(MHz)	Center frequency of the non-Wi-Fi device.

Item	Description
Non-Wi-Fi device bandwidth(KHz)	Bandwidth of the non-Wi-Fi device.
Non-Wi-Fi device duty(%)	Duty cycle of the non-Wi-Fi device.
Non-Wi-Fi device interfere level	Interference level of the non-Wi-Fi device. The value ranges from 0 to 3. A larger value indicates stronger interference.

11.5.6 spectrum-analysis enable

Function

(AP group radio view) The **spectrum-analysis enable** command enables spectrum analysis on a specified radio in an AP group.

(AP group radio view) The **undo spectrum-analysis enable** command disables spectrum analysis on a specified radio in an AP group.

(AP radio view) The **spectrum-analysis enable** command enables spectrum analysis on a specified AP radio.

(AP radio view) The **undo spectrum-analysis enable** command restores the AP radio configuration to that in the AP group radio view.

By default, spectrum analysis is disabled on an AP radio.

Format

spectrum-analysis enable

undo spectrum-analysis enable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If interference exists on a WLAN, enable spectrum analysis on AP radios to implement spectrum scanning, sampling, and analysis on the wireless signals. The

spectrum analysis function helps identify non-Wi-Fi interference on the WLAN and locate non-Wi-Fi devices to optimize the WLAN.

Precautions

If the WDS or Mesh service is configured on a radio, the command cannot be executed in the radio view.

Example

Enable spectrum analysis on radio 0 of the AP with ID 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] spectrum-analysis enable
```

11.5.7 spectrum-analysis non-wifi-device aging-time

Function

The **spectrum-analysis non-wifi-device aging-time** command configures the aging time for non-Wi-Fi device information during spectrum analysis.

The **undo spectrum-analysis non-wifi-device aging-time** command restores the default aging time for non-Wi-Fi device information during spectrum analysis.

By default, the aging time for non-Wi-Fi device information is 3 minutes.

Format

spectrum-analysis non-wifi-device aging-time *aging-time*

undo spectrum-analysis non-wifi-device aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time for non-Wi-Fi device information.	The value is an integer that ranges from 1 to 30, in minutes.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a spectrum analysis server is configured using the **spectrum-analysis server** command, the AC stores information about analyzed non-Wi-Fi device information. If information about a non-Wi-Fi device is not reported again within the aging time configured using the **spectrum-analysis non-wifi-device aging-time** command, the AC adds the non-Wi-Fi device to the historical list. You can run the **display wlan non-wifi-device history** command to check information about non-Wi-Fi devices in the historical list.

Precautions

Currently, the device cannot identify different devices of the same type. For example, when the device detects Bluetooth devices A and B, the device can only record them as Bluetooth devices and update the detection time of the Bluetooth device.

Example

Set the aging time for non-Wi-Fi device information to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] spectrum-analysis non-wifi-device aging-time 5
```

11.5.8 spectrum-analysis server

Function

The **spectrum-analysis server** command specifies the IP address and port number of a spectrum server.

The **undo spectrum-analysis server** command deletes the specified IP address and port number of a spectrum server.

By default, no spectrum server is configured.

Format

spectrum-analysis server ip-address *ip-address* **port** *port-number* [**via-ac ac-port** *ac-port-number*]

undo spectrum-analysis server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IPv4 address of a spectrum server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number (UDP port number) of a spectrum server.	The value is an integer that ranges from 1 to 65535. **NOTE** The port number of eSight is 32181, and that of iMaster NCE-CampusInsight is 27371.

Parameter	Description	Value
via-ac	Configures the AP to report spectrum data to the spectrum server via the AC.	-
ac-port *ac-port-number*	Specifies the port number used by the AC to receive spectrum data (in UDP packets) from the AP.	The value is an integer that ranges from 5000 to 65535.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After collecting the spectrum data, an AP encapsulates the collected data into UDP packets and sends the packets to the spectrum server. The spectrum server draws a spectrum and displays the spectrum information of the detected non-Wi-Fi devices to users through images.

- If the AP uploads the collected data directly to the spectrum server, you do not need to configure the **via-ac ac-port** *ac-port-number* command.
- If the AP uploads the collected data to the spectrum server via the AC, configure the **via-ac ac-port** *ac-port-number* command.
- If no spectrum server is available, to view the spectrum in the web system of an AC, specify a valid IP address and port number for the spectrum server (which do not take effect) and configure the **via-ac ac-port** *ac-port-number* command.

Follow-up Procedure

Run the **spectrum-report** { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* command to enable the function of reporting spectrum data on an AP radio.

Example

Set the IP address and port number of a spectrum server to 10.137.43.4 and 27371, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] spectrum-analysis server ip-address 10.137.43.4 port 27371
```


11.5.9 spectrum-analysis source

Function

The **spectrum-analysis source** command configures the source IP address of packets sent by the AC to a spectrum server.

The **undo spectrum-analysis source** command deletes the configured source IP address of packets sent by the AC to a spectrum server.

By default, the AC uses the IP address of the outbound interface on the matched route as the source IP address of packets sent to a spectrum server.

Format

spectrum-analysis source ip-address *ip-address*

undo spectrum-analysis source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the source IPv4 address of packets sent by the AC to a spectrum server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, when sending data packets to a spectrum server, the AC uses the IP address of the outbound interface on the matched route between them to communicate with the spectrum server.

After the source IP address is configured using the **spectrum-analysis source** command, the AC uses this IP address to communicate with the spectrum server.

Precautions

- Ensure that the AC's IP address manually configured on the spectrum server is the same as that configured using the **spectrum-analysis source** command.
- The configured source IP address must exist on the AC and is routable with the spectrum server.

Example

Configure 10.102.25.23 as the source IP address of packets sent by the AC to a spectrum server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] spectrum-analysis source ip-address 10.102.25.23
```

11.5.10 spectrum-report

Function

The **spectrum-report** command enables the function of reporting spectrum data on an AP radio.

The **undo spectrum-report** command disables the function of reporting spectrum data on an AP radio.

By default, the function of reporting spectrum data is disabled on an AP radio.

Format

spectrum-report { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

undo spectrum-report { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name. The AP name and radio ID identify a radio.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID. The AP ID and radio ID identify a radio.	The AP ID must exist.

Parameter	Description	Value
radio *radio-id*	Specifies a radio ID.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: • AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 • AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T • AirEngine 8771-X1T
all	Specifies all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of reporting spectrum data is enabled on an AP radio, the AP encapsulates collected data into UDP packets and sends the packets to the spectrum server. After receiving the data, the spectrum server analyzes the data and then displays radio information of non-Wi-Fi devices to users through images or tables.

Prerequisites

The spectrum analysis function has been enabled on a radio using the **spectrum-analysis enable** command.

Follow-up Procedure

Run the **spectrum-analysis server** command in the spectrum profile view to specify the IP address and port number of the spectrum server.

Precautions

The **spectrum-report** command becomes invalid after the AC restarts, and needs to be configured again.

Example

Enable the function of reporting spectrum data on radio 0 of the AP named **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] spectrum-report ap-name test radio 0
```

11.5.11 reset wlan non-wifi-device

Function

The **reset wlan non-wifi-device** command clears information about detected non-Wi-Fi devices.

Format

reset wlan non-wifi-device { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Clears information about the non-Wi-Fi devices detected by all APs.	-
ap-name *ap-name*	Clears information about the non-Wi-Fi devices detected by a specified AP name.	The AP name must exist.
ap-id *ap-id*	Clears information about the non-Wi-Fi devices detected by a specified AP ID.	The AP ID must exist.

Parameter	Description	Value
radio *radio-id*	Clears information about the non-Wi-Fi devices detected by a specified AP radio.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: • AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 • AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T • AirEngine 8771-X1T

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before re-collecting information about detected non-Wi-Fi devices in a period, you can run this command to clear existing information so that the AC can re-collect information.

Prerequisites

The spectrum analysis function has been enabled on a radio.

Impact

The cleared non-Wi-Fi device information cannot be restored. Exercise caution when you run this command. After the command is run, you can run the **display wlan non-wifi-device history** command to view related information.

Example

Clear information about the non-Wi-Fi devices detected by all APs.

```
<HUAWEI> reset wlan non-wifi-device all
```


11.5.12 reset wlan non-wifi-device history

Function

The **reset wlan non-wifi-device history** command clears information about non-Wi-Fi devices in the historical list.

Format

reset wlan non-wifi-device history { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Clears information about all the non-Wi-Fi devices in the historical list.	-
ap-name *ap-name*	Clears information about the non-Wi-Fi devices detected by a specified AP name in the historical list.	The AP name must exist.
ap-id *ap-id*	Clears information about the non-Wi-Fi devices detected by a specified AP ID in the historical list.	The AP ID must exist.
radio *radio-id*	Clears information about the non-Wi-Fi devices detected by a specified AP radio in the historical list.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: • AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 • AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T • AirEngine 8771-X1T

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to clear information about non-Wi-Fi devices in the historical list.

Example

Clear information about the non-Wi-Fi devices detected by all APs in the historical list.

```
<HUAWEI> reset wlan non-wifi-device history all
```

11.6 WLAN Roaming Commands

11.6.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.6.2 beacon disable

Function

The **beacon disable** command disables an RU from sending Beacon frames.

The **undo beacon disable** command allows an RU to send Beacon frames.

By default, an RU is allowed to send Beacon frames.

NOTE

This command does not take effect for the following APs:

- AirEngine 9700D-S
- AirEngine X77X
- AirEngine X76X (including RUs)

Format

beacon disable

undo beacon disable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure synchronization of Beacon frames in scenarios with densely deployed RUs, you can run the **beacon disable** command to disable some RUs from sending Beacon frames. This configuration is recommended on a network enabled with agile distributed SFN roaming. In other scenarios, the default configuration is recommended.

Precautions

Disabling an RU from sending Beacon frames may cause STAs to go offline due to a failure to receive Beacon frames.

Example

Disable an RU from sending Beacon frames.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] beacon disable
Warning: This configuration is recommended in SFN roaming scenarios. This action
 may cause service interruption. Continue? [Y/N]Y
```

11.6.3 capwap dtls inter-controller control-link encrypt

Function

The **capwap dtls inter-controller control-link encrypt** command configures DTLS encryption for an inter-AC control tunnel.

The **undo capwap dtls inter-controller control-link encrypt** command restores the default configuration of DTLS encryption for an inter-AC control tunnel.

By default, DTLS encryption for an inter-AC control tunnel is disabled.

Format

capwap dtls inter-controller control-link encrypt

undo capwap dtls inter-controller control-link encrypt

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

At the discovery stage of inter-AC tunnel establishment, the AC obtains the IP address of another AC through the discovery mechanism. After that, the ACs enter the DTLS negotiation stage, in which the ACs use DTLS to set up a tunnel and encrypt UDP packets forwarded in the tunnel.

After this command is executed, packets transmitted over an inter-AC control tunnel are encrypted using DTLS. The ACs implement DTLS negotiation in PSK encryption mode. If DTLS negotiation fails, the inter-AC tunnel cannot be set up.

Precautions

If you modify the DTLS configuration after an inter-AC tunnel is set up, the modification takes effect at the next tunnel setup.

When DTLS encryption is enabled for an inter-AC control tunnel on the server-side AC, the inter-AC tunnel can be set up only when this function is enabled on client-side AC. When DTLS encryption is enabled for an inter-AC control tunnel on the client-side AC, the inter-AC tunnel can be set up if even this function is disabled on the server-side AC.

Before enabling this function, run the **capwap dtls inter-controller psk** command to configure a PSK.

Example

Enable DTLS encryption for an inter-AC control tunnel.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls inter-controller control-link encrypt
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue?
[Y/N]:y
```

11.6.4 capwap dtls inter-controller psk

Function

The **capwap dtls inter-controller psk** command configures a pre-shared key (PSK) for DTLS encryption of inter-AC tunnels.

By default, no PSK is configured for DTLS encryption.

Format

capwap dtls inter-controller psk *psk-value*

Parameters

Parameter	Description	Value
psk-value	Specifies a PSK for DTLS encryption.	The value is string of 48 or 68 characters in ciphertext (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'Ol*Gmt.V(%^%#**) or a string of 8 to 32 characters in plaintext (for example, **YsHsjx_202206**). The key must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios such as inter-AC roaming and centralized license control, ACs synchronize data and forward packets through CAPWAP tunnels. If DTLS encryption for inter-AC tunnels is configured, DTLS negotiation is initiated when an AC negotiates with the peer AC to establish a CAPWAP link. Subsequent UDP packets are encrypted using DTLS to improve transmission security.

DTLS supports PSK encryption. When a PSK is used for DTLS encryption, you can use this command to change the value of the PSK on the AC.

Follow-up Procedure

Run the **capwap dtls inter-controller control-link encrypt** command to enable DTLS encryption for inter-AC control tunnels.

Precautions

If you modify the PSK after an inter-AC tunnel is set up, the modification takes effect at the next tunnel setup.

DTLS encryption must be enabled on ACs at both ends of the tunnel, and the ACs must have the same PSK.

It is recommended that you configure the same PSK on the ACs at both ends before enabling DTLS encryption. In this way, the ACs have the same PSK. If you enable DTLS encryption but the ACs have different PSKs, DTLS negotiation fails. As a result, the tunnel cannot be set up between the ACs.

NOTE

To implement roaming between ACs running different versions, you must manually configure the same PSK on the ACs in the mobility group.

Example

Configure the PSK **YsHsjx_202206** for DTLS encryption of an inter-AC tunnel.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls inter-controller psk YsHsjx_202206
```

11.6.5 capwap inter-controller sensitive-info psk

Function

The **capwap inter-controller sensitive-info psk** command configures a pre-shared key (PSK) used for encrypting sensitive information between ACs.

The **undo capwap inter-controller sensitive-info psk** command deletes the configured PSK used for encrypting sensitive information between ACs.

By default, no PSK is configured for encrypting sensitive information between ACs.

Format

capwap inter-controller sensitive-info psk *key-value*

undo capwap inter-controller sensitive-info psk

Parameters

Parameter	Description	Value
key-value	Specifies a PSK for encrypting sensitive information between ACs.	The value is a string of 6 to 32 case-sensitive characters without question marks (?) or spaces. For a plaintext PSK, the length must be 48 or 68 bits. If the string is enclosed in double quotation marks ("), the string can contain spaces. **NOTE** For security purposes, it is recommended that the PSK contain at least eight characters from at least two of the following types: uppercase letters, lowercase letters, digits, and special characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In multi-AC scenarios where inter-AC communication is established through CAPWAP tunnels (such as inter-AC roaming and centralized license control), ACs may need to exchange sensitive information such as the user name and password. You can configure a PSK to protect sensitive data transmitted between ACs.

Precautions

- Ensure that the ACs have the same PSK. Otherwise, the CAPWAP tunnel cannot be set up between the ACs.
- This function must be configured on the ACs at both ends of a CAPWAP tunnel, and the ACs must have the same PSK. Otherwise, the CAPWAP tunnel cannot be set up between the ACs.

Example

Set the PSK used for encrypting sensitive information between ACs to **YsHsjx_202206**.


```
<HUAWEI> system-view
[HUAWEI] capwap inter-controller sensitive-info psk YsHsjx_202206
Warning: The ACs must have the same configuration. Otherwise, the link between them cannot be set up.
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue?
[Y/N]:Y
```

11.6.6 cts delay

Function

The **cts delay** command sets a delay for RUs to respond to STAs with CTS packets.

The **undo cts delay** command deletes the delay configured for RUs to respond to STAs with CTS packets.

By default, RUs respond to STAs with CTS packets with no delay.

Format

cts delay *delay-time*

undo cts delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay time after which RUs respond to STAs with CTS packets.	The value is an integer that ranges from 1 to 255, in microseconds.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

After the **undo cts disable** command is executed to enable RUs to respond to STAs with CTS packets, you can configure a response delay. When multiple RUs respond to STAs with CTS packets, you can configure the delay for some RUs to prevent conflicts.

Example

Set the delay for RUs to respond to STAs with CTS packets to 60 microseconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
```



```
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] undo cts disable
[HUAWEI-wlan-radio-1/0] cts delay 60
```

11.6.7 cts disable

Function

The **cts disable** command disables RUs from responding to STAs with CTS packets.

The **undo cts disable** command enables RUs to respond to STAs with CTS packets.

By default, RUs are enabled to respond to STAs with CTS packets.

Format

cts disable

undo cts disable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent CTS conflicts in scenarios with densely deployed RUs, you can run the **cts disable** command to disable some RUs from responding to STAs with CTS packets. This configuration is recommended on a network enabled with agile distributed SFN roaming. In other scenarios, the default configuration is recommended.

Precautions

Disabling RUs from responding to STAs with CTS packets may cause STAs to go offline due to a failure to receive CTS packets.

This command does not take effect on the R250D, R250D-E, R251D, R251D-E, or R450D.

Example

Disable RUs from responding to STAs with CTS packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
```



```
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] cts disable
Warning: This configuration is recommended in SFN roaming scenarios. This action
 may cause service interruption. Continue? [Y/N]y
```

11.6.8 display mobility-group

Function

The **display mobility-group** command displays configurations of mobility groups.

Format

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

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a mobility group.	The mobility group name must already exist.
all	Specifies all mobility groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mobility-group** command to view configurations of mobility groups.

Example

Display configurations of the mobility group **hello**.

```
<HUAWEI> display mobility-group name hello
--------------------------------------------------------------------------------
State       IP address                  Description
--------------------------------------------------------------------------------
normal       192.168.10.1                 -
normal       192.168.10.2                 -
fault       192.168.10.3                -
--------------------------------------------------------------------------------
Total: 3
```


Table 11-160 Description of the **display mobility-group** command output

Item	Description
State	Status of the CAPWAP links between members in the mobility group and the local AC. • normal: The CAPWAP links are working properly. • fault: The CAPWAP links are disconnected. • vmiss: The versions of members in the mobility group and the local AC do not match. • -: No CAPWAP link is established between members in the mobility group and the local AC.
IP address	AC's IP address.
Description	Description of the AC.

Display configurations of all mobility groups.

```
<HUAWEI> display mobility-group all
-------------------------------------------------------------------------------
Group name
-------------------------------------------------------------------------------
group1
mobility-test
-------------------------------------------------------------------------------
Total: 2
```

Table 11-161 Description of the **display mobility-group all** command output

Item	Description
Group name	Mobility group name.

11.6.9 display station roam-statistics

Function

The **display station roam-statistics** command displays STA roaming statistics.

Format

display station roam-statistics [**ap-name** *ap-name* | **ap-id** *ap-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays statistics about STAs associated with the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays statistics about STAs associated with the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display station roam-statistics** command to view STA roaming statistics.

- If no parameter is specified, roaming statistics about all associated STAs are displayed.
- If an AP name or ID is specified, roaming statistics about all STAs associated with the AP are displayed.

Example

Display roaming statistics about all STAs.

```
<HUAWEI> display station roam-statistics
-------------------------------------------------------------------------------
 Online STAs                                    :0
 Online roaming stations                        :0
-------------------------------------------------------------------------------
```

Table 11-162 Description of the **display station roam-statistics** command output

Item	Description
Online STAs	Number of online STAs.
Online roaming stations	Number of online roaming STAs.

Display roaming statistics about STAs associated with a specified AP.

```
<HUAWEI> display station roam-statistics ap-name N1-2
-------------------------------------------------------------------------------
```



```
Online STAs                                  :0
Online roaming stations                      :0
Online L3 roam stations                      :0
L3 roam-in                                   :0
L3 roam-out                                  :0
------------------------------------------------------------------------------
```

Table 11-163 Description of the **display station roam-statistics ap-name** *ap-name* command output

Item	Description
Online STAs	Number of online STAs.
Online roaming stations	Number of online roaming STAs.
Online L3 roam stations	Number of Layer 3 roaming STAs.
L3 roam-in	Number of STAs roaming from another AP to the local AP.
L3 roam-out	Number of STAs roaming from the local AP to another AP.

11.6.10 display station roam-track

Function

The **display station roam-track** command displays the roaming track of a STA.

Format

display station roam-track sta-mac *mac-address*

Parameters

Parameter	Description	Value
sta-mac *mac-address*	Specifies the MAC address of a specified STA.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During the roaming process of a STA, the AC records the STA's roaming track (that is, information about the APs that the STA connects to). You can run the **display station roam-track** command to view the roaming track of the STA.

Example

Display the roaming track of the STA with the MAC address 00e0-fc00-0001.

```
<HUAWEI> display station roam-track sta-mac 00e0-fc00-0001
Access SSID:test
Rx/Tx:link receive rate/link transmit rate(Mbps)
s: Same Frequency Network c:PMK Cache Roam
r:802.11r Roam d:802.11r over ds Roam p:proprietary 802.11r Roam
-------------------------------------------------------------------------------
L2/L3          AP-AC IP              AC-AC IP            AP name              Radio ID
BSSID          TIME                  In/Out RSSI         Out Rx/Tx
-------------------------------------------------------------------------------
--             192.168.109.1         -                   test1                1
00e0-fc76-e360  2015-01-12/16:52:58    -51/-48             46/13
L2             192.168.109.1         -                   test2                1
00e0-fc74-9640  2015-01-12/16:55:45    -58/-               -/-
-------------------------------------------------------------------------------
Number: 1
```

Table 11-164 Description of the **display station roam-track** command output

Item	Description
Access SSID	SSID associated with a STA.
Rx/Tx	Negotiated rate between the STA and AP.
L2/L3	Roaming mode. Suffix description: • s: agile distributed SFN roaming • c: PMK fast roaming. • r: 802.11r fast roaming (over-the-air mode) • d: 802.11r fast roaming (standard over-the-DS mode) • p: 802.11r fast roaming (proprietary over-the-DS mode)
AP-AC IP	CAPWAP source IP address used by the AC that the STA is associated with for setting up a CAPWAP tunnel with the AP that the STA is associated with.
AC-AC IP	CAPWAP source IP address used by the AC that the STA is associated with for setting up CAPWAP tunnels with other ACs.

Item	Description
AP name	Name of an AP that the STA is associated with.
Radio ID	ID of a radio that the STA is associated with.
BSSID	BSSID of an AP that the STA is associated with.
TIME	Time duration when the STA is associated with an AP.
In/Out RSSI	RSSI of the AP that the STA is associated with and RSSI of the AP away from which the STA has left.
Out Rx/Tx	Negotiated rate of the STA when it disconnects from an AP.
Number	Number of STA roaming tracks.

11.6.11 dot11r enable

Function

The **dot11r enable** command enables 802.11r.

The **undo dot11r enable** command disables 802.11r.

By default, 802.11r is disabled.

Format

dot11r enable [**over-the-ds**]

undo dot11r enable

Parameters

Parameter	Description	Value
over-the-ds	Indicates 802.11r roaming in over-the-DS mode.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During roaming, the STA needs to be reauthenticated and re-negotiate a key, so services are interrupted for a short period of time. You can enable 802.11r to reduce the number of information exchanges during roaming, thus reducing latency.

Precautions

- Security policies supported by 802.11r include open system, WPA2+PSK+AES, WPA2+PPSK+AES, and WPA2+802.1X+AES.
- The 802.11r and Protected Management Frame (PMF) functions are mutually exclusive. If the 802.11r function has been configured, the PMF function cannot be configured.
- Over-the-DS 802.11r roaming across ACs is not supported.

Example

Enable the 802.11r function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dot11r enable
```

11.6.12 dot11r proprietary

Function

The **dot11r proprietary** command enables the Huawei's proprietary 802.11r function (device-pipe synergy roaming).

The **undo dot11r proprietary** command disables the Huawei's proprietary 802.11r function.

By default, Huawei's proprietary 802.11r function is disabled.

Format

dot11r proprietary

undo dot11r proprietary

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to the characteristics of Wi-Fi and different behaviors of different terminals on the WLAN, the actual roaming experience for the terminals varies. The roaming experience for latency-sensitive services such as audio, video, and gaming cannot be guaranteed. Roaming optimization policies are different for terminals and APs and may conflict with each other. Therefore, simply optimization for terminals or APs cannot solve the problem. APs are optimized for Huawei's terminals running EMUI 10.0 or later. After the Huawei's proprietary 802.11r function is enabled, APs can carry the interworking IE in Beacon and Probe Response frames and perform roaming negotiation with Huawei terminals based on the specified frame format and interaction action. This function implements mutual trust and interworking between devices and pipes, reduces resource overheads during roaming negotiation, and effectively improves roaming experience.

Precautions

- Security policies supported by 802.11r include open system, WPA2+PSK+AES, WPA2+PPSK+AES, and WPA2+802.1X+AES.
- The 802.11r and Protected Management Frame (PMF) functions are mutually exclusive. If the 802.11r function has been configured, the PMF function cannot be configured.

Example

Enable the Huawei's proprietary 802.11r function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dot11r proprietary
```

11.6.13 dot11r reassociate-timeout

Function

The **dot11r reassociate-timeout** command sets the 802.11r reassociation timeout period.

The **undo dot11r reassociate-timeout** command restores the default 802.11r reassociation timeout period.

By default, the 802.11r reassociation timeout period is 1s.

Format

dot11r reassociate-timeout *time*

undo dot11r reassociate-timeout

Parameters

Parameter	Description	Value
reassociate-timeout *time*	Specifies the reassociation timeout period. After successful authentication, if the STA does not initiate a reassociation request within this period, the roaming fails.	The value is an integer that ranges from 1 to 10, in seconds.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During roaming, the STA needs to be reauthenticated and re-negotiate a key, so services are interrupted for a short period of time. You can enable 802.11r to reduce the number of information exchanges during roaming, thus reducing latency.

Precautions

- Security policies supported by 802.11r include open system, WPA2+PSK+AES, WPA2+PPSK+AES, and WPA2+802.1X+AES.
- The 802.11r and Protected Management Frame (PMF) functions are mutually exclusive. If the 802.11r function has been configured, the PMF function cannot be configured.

Example

Set the 802.11r reassociation timeout period to 3s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dot11r reassociate-timeout 3
```

11.6.14 member (mobility group view)

Function

The **member** command adds a member AC to a mobility group.

The **undo member** command deletes a member AC from a mobility group.

By default, no member AC is added to a mobility group.

Format

member ip-address *ipv4-address* [**description** *description*]

undo member ip-address *ipv4-address*

Parameters

Parameter	Description	Value
ip-address *ipv4-address*	Specifies the IPv4 address of a mobility group member.	The value is in dotted decimal notation.
description *description*	Description of a mobility group member.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

mobility group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a STA to roam between ACs, run the **mobility-group name** *group-name* command to configure a mobility group. The STA can roam between the ACs in the group. You can run the **member** command to add a member AC to the mobility group.

Precautions

An AC can be added only to one mobility group.

Example

Add the AC with IPv4 address 192.168.100.1 to the mobility group **mobility**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mobility-group name mobility
[HUAWEI-mc-mg-mobility] member ip-address 192.168.100.1
```

Remove the AC with IPv4 address 192.168.100.1 from the mobility group **mobility**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mobility-group name mobility
[HUAWEI-mc-mg-mobility] undo member ip-address 192.168.100.1
```


11.6.15 mobility-group

Function

The **mobility-group** command creates a mobility group and displays the mobility group view. If the specified mobility group exists, you can directly enter the specified mobility group view.

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

By default, no mobility group is created.

Format

mobility-group name *group-name*

undo mobility-group { **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a mobility group.	The value is a string of 1 to 31 characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Indicates all mobility groups.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

STAs can roam between ACs in a mobility group. You can run the **mobility-group** command to create a mobility group and add required ACs to the group.

Follow-up Procedure

Run the **member ip-address** *ipv4-address* [**description** *description*] command to add member ACs to the mobility group.

Example

Create a mobility group named **mobility** and display the mobility group view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mobility-group name mobility
[HUAWEI-mc-mg-mobility]
```

Delete a mobility group.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] undo mobility-group name mobility
Warning:The mobility group will be deleted, are you sure to continue?[Y/N]:y
```

Delete all mobility groups.

11.6.16 mobility-server local

Function

The **mobility-server local** command configures a local IP address for setting up links between ACs in a mobility group.

The **undo mobility-server local** command deletes the local IP address for setting up links between ACs in a mobility group.

By default, no local IP address is configured for setting up links between ACs in a mobility group.

Format

mobility-server local ip-address *ipv4-address*

undo mobility-server local

Parameters

Parameter	Description	Value
ip-address *ipv4-address*	Specifies an IPv4 address for setting up links between ACs in a mobility group.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In inter-AC roaming scenarios, you need to specify a local IP address for STAs to roam between ACs.

Precautions

The specified IP address must be the same as the CAPWAP source IP address. When multiple CAPWAP source addresses are configured, only one can be specified as the local IP address for setting up links between ACs.

Example

Configure 192.168.10.1 as the local IP address for setting up links between ACs in a mobility group.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mobility-server local ip-address 192.168.10.1
```

11.6.17 sfn-roam enable

Function

The **sfn-roam enable** command enables agile distributed SFN roaming.

The **undo sfn-roam enable** command disables agile distributed SFN roaming.

By default, agile distributed SFN roaming is disabled.

Format

sfn-roam enable

undo sfn-roam enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the agile distributed Wi-Fi networking, some scenarios require high network connection stability, such as healthcare scenarios. In this case, you can run the **sfn-roam enable** command to enable agile distributed SFN roaming. All RUs are deployed to work on the same channel and use the same BSSID for communicating with STAs. When the STAs move within the signal coverage of the same SSID, they are not aware of roaming and services are not interrupted.

Example

Enable agile distributed SFN roaming.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] sfn-roam enable
Warning: This feature requires that radios work on the same channel. Enabling th
is feature will disable the channel calibration, channel scanning, and smart roa
ming functions on the AP and disconnect STAs connected to the VAP. Open, WEP, an
d WAPI encryption modes are not supported. The PSK + WPA2 mode is recommended. A
 radio allows SFN to be enabled only for one VAP. Continue?[Y/N]:y
```

11.6.18 sfn-roam report-interval

Function

The **sfn-roam report-interval** command sets an interval at which RUs report STA RSSIs.

The **undo sfn-roam report-interval** command restores the default interval at which RUs report STA RSSIs.

By default, RUs report STA RSSIs to the central AP at an interval of 400 milliseconds.

Format

sfn-roam report-interval *report-interval-value*

undo sfn-roam report-interval

Parameters

Parameter	Description	Value
report-interval-value	Specifies an interval for RUs to report STA RSSIs.	The value is an integer that ranges from 200 to 1000, in milliseconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The interval at which RUs report STA RSSIs helps you adjust the roaming sensitivity. A shorter interval indicates a higher sensitivity. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent

roaming handovers, affecting system performance. This interval must be smaller than the decision period for agile distributed SFN roaming.

Example

Set the interval for RUs to report the STA RSSI to 500 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam report-interval 500
```

11.6.19 sfn-roam roam-check better-times

Function

The **sfn-roam roam-check better-times** command sets the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU.

The **undo sfn-roam roam-check better-times** command restores the default number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU.

By default, the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU is 2.

Format

sfn-roam roam-check better-times *better-times*

undo sfn-roam roam-check better-times

Parameters

Parameter	Description	Value
better-times	Specifies the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU.	The value is an integer that ranges from 1 to 32.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can adjust the roaming sensitivity by setting the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU. A roaming handover occurs when the RSSI of a surrounding RU is higher than that of the

local RU for the specified times within the roaming decision period. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance.

Example

Set the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check better-times 5
```

11.6.20 sfn-roam roam-check check-interval

Function

The **sfn-roam roam-check check-interval** command sets the decision period for agile distributed SFN roaming.

The **undo sfn-roam roam-check check-interval** command restores the default decision period for agile distributed SFN roaming.

The default decision period for agile distributed SFN roaming is 700 milliseconds.

Format

sfn-roam roam-check check-interval *check-interval-value*

undo sfn-roam roam-check check-interval

Parameters

Parameter	Description	Value
check-interval-value	Specifies the decision period for agile distributed SFN roaming.	The value is an integer that ranges from 300 to 1500, in milliseconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The decision period for agile distributed SFN roaming helps you adjust the roaming sensitivity. A shorter period indicates a higher sensitivity. A large value

causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance. The default value is recommended. Ensure that the interval at which RUs report STA RSSIs is smaller than the decision period for agile distributed SFN roaming.

Example

Set the default decision period for agile distributed SFN roaming to 800 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check check-interval 800
```

11.6.21 sfn-roam roam-check gap-rssi

Function

The **sfn-roam roam-check gap-rssi** command sets the RSSI gap for agile distributed SFN roaming RUs.

The **undo sfn-roam roam-check gap-rssi** command restores the default RSSI gap for agile distributed SFN roaming RUs.

The default RSSI gap for agile distributed SFN roaming RUs is 6 dB.

Format

sfn-roam roam-check gap-rssi *gap-rssi*

undo sfn-roam roam-check gap-rssi

Parameters

Parameter	Description	Value
gap-rssi	Specifies the RSSI gap for agile distributed SFN roaming RUs.	The value is an integer that ranges from 1 to 32, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The RSSI gap for agile distributed SFN roaming RUs helps you adjust the roaming sensitivity. A roaming handover occurs when the RSSI gap between the local RU

and a surrounding RU reaches the specified value. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance.

Example

Set the RSSI gap for agile distributed SFN roaming RUs to 10 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check gap-rssi 10
```

11.6.22 sfn-roam roam-check high-threshold

Function

The **sfn-roam roam-check high-threshold** command sets the upper RSSI threshold for agile distributed SFN roaming.

The **undo sfn-roam roam-check high-threshold** command restores the default upper RSSI threshold for agile distributed SFN roaming.

By default, the upper RSSI threshold for agile distributed SFN roaming is -55 dBm.

Format

sfn-roam roam-check high-threshold *high-threshold-value*

undo sfn-roam roam-check high-threshold

Parameters

Parameter	Description	Value
high-threshold-value	Specifies the upper RSSI threshold for agile distributed SFN roaming.	The value is an integer that ranges from -60 to -45, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the STA RSSI threshold to control the sensitivity of agile distributed SFN roaming and prevent STAs from frequently roaming at radio borders of RUs. A

roaming handover occurs when the total number of records in the following conditions exceeds the value specified by the **sfn-roam roam-check better-times** command:

- When the HAP detects that the STA RSSI is lower than the lower threshold: The central AP makes a record if the SNR of the FAP is higher than that of the HAP.
- When the HAP detects that the STA RSSI is between the upper and lower thresholds: The central AP makes a record if the SNR of the FAP is 3 dB higher than that of the HAP.
- When the HAP detects that the STA RSSI is higher than the upper threshold: The central AP makes a record if the SNR of the FAP is 5 dB higher than that of the HAP.

Precautions

The lower RSSI threshold for agile distributed SFN roaming must be no higher than the upper threshold.

Example

Set the upper RSSI threshold for agile distributed SFN roaming to -50 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check high-threshold -50
```

11.6.23 sfn-roam roam-check low-threshold

Function

The **sfn-roam roam-check low-threshold** command sets the lower RSSI threshold for agile distributed SFN roaming.

The **undo sfn-roam roam-check low-threshold** command restores the default lower RSSI threshold for agile distributed SFN roaming.

By default, the lower RSSI threshold for agile distributed SFN roaming is -60 dBm.

Format

sfn-roam roam-check low-threshold *low-threshold-value*

undo sfn-roam roam-check low-threshold

Parameters

Parameter	Description	Value
low-threshold-value	Specifies the lower RSSI threshold for agile distributed SFN roaming.	The value is an integer that ranges from -70 to -55, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the STA RSSI threshold to control the sensitivity of agile distributed SFN roaming and prevent STAs from frequently roaming at radio borders of RUs. A roaming handover occurs when the total number of records in the following conditions exceeds the value specified by the **sfn-roam roam-check better-times** command:

- When the HAP detects that the STA RSSI is lower than the lower threshold: The central AP makes a record if the SNR of the FAP is higher than that of the HAP.
- When the HAP detects that the STA RSSI is between the upper and lower thresholds: The central AP makes a record if the SNR of the FAP is 3 dB higher than that of the HAP.
- When the HAP detects that the STA RSSI is higher than the upper threshold: The central AP makes a record if the SNR of the FAP is 5 dB higher than that of the HAP.

Precautions

The lower RSSI threshold for agile distributed SFN roaming must be no higher than the upper threshold.

Example

Set the lower RSSI threshold for agile distributed SFN roaming to -65 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check low-threshold -65
```

11.6.24 sfn-roam roam-check rssi-accumulate

Function

The **sfn-roam roam-check rssi-accumulate** command sets the cumulative RSSI change threshold for agile distributed SFN roaming STAs.

The **undo sfn-roam roam-check rssi-accumulate** command restores the default cumulative RSSI change threshold for agile distributed SFN roaming STAs.

By default, the cumulative RSSI change threshold of agile distributed SFN roaming STAs is 8 dB.

Format

sfn-roam roam-check rssi-accumulate threshold *rssi-accumulate-value*

undo sfn-roam roam-check rssi-accumulate

Parameters

Parameter	Description	Value
threshold *rssi-accumulate-value*	Specifies the cumulative RSSI change threshold for agile distributed SFN roaming STAs.	The value is an integer that ranges from 1 to 32, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The cumulative RSSI change threshold of agile distributed SFN roaming STAs helps you adjust the roaming sensitivity. A roaming handover occurs when the cumulative RSSI change value reaches the specified threshold. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance.

Example

Set the cumulative RSSI change threshold for agile distributed SFN roaming STAs to 10 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check rssi-accumulate threshold 10
```

11.6.25 sfn-roam roam-check sta-holding times

Function

The **sfn-roam roam-check sta-holding times** command sets the number of STA holding times for agile distributed SFN roaming.

The **undo sfn-roam roam-check sta-holding times** command restores the default number of STA holding times for agile distributed SFN roaming.

By default, the number of STA holding times for agile distributed SFN roaming is 3.

Format

sfn-roam roam-check sta-holding times *sta-holding-times*

undo sfn-roam roam-check sta-holding times

Parameters

Parameter	Description	Value
sta-holding-times	Specifies the number of STA holding times for agile distributed SFN roaming.	The value is an integer that ranges from 1 to 32.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

To prevent frequent agile distributed SFN roaming handovers, you can specify a proper number of STA holding times. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance.

Example

Set the number of STA holding times for agile distributed SFN roaming to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check sta-holding times 5
```

11.6.26 inter-ac roam disable

Function

The **inter-ac roam disable** command disables inter-AC roaming.

The **undo inter-ac roam disable** command enables inter-AC roaming.

By default, inter-AC roaming is enabled.

Format

inter-ac roam disable

undo inter-ac roam disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

If STAs roam from one AC to another, they have to be re-authenticated to access the network. To limit the STA roaming scope within an AC, you can run the **inter-ac roam disable** command to disable inter-AC roaming.

Example

Disable inter-AC roaming.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] inter-ac roam disable
```

11.7 WLAN QoS Configuration Commands

11.7.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.7.2 airtime-fair-schedule enable

Function

The **airtime-fair-schedule enable** command enables airtime fair scheduling on an AP radio.

The **undo airtime-fair-schedule enable** command disables airtime fair scheduling on an AP radio.

By default, airtime fair scheduling is disabled on an AP radio.

Format

airtime-fair-schedule enable

undo airtime-fair-schedule enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a WLAN, the physical layer rates of users have great differences due to different radio modes supported by the terminals or radio environment where the terminals reside. If the users with lower physical layer rates occupy wireless channels for a long period, user experience of the entire WLAN is affected. Airtime fair scheduling calculates the channel occupation time of users transmitting the same service and preferentially schedules resources for the users who occupy the wireless channel for a shorter period. This ensures fairness in channel usage.

After airtime fair scheduling is enabled, the device collects statistics on the channel occupation time used by users connected to the same radio for sending packets, creates the mapping table for the channel occupation time of each user in accumulated mode, and establishes a sorted link table based on the time in an ascending order. Based on the mapping table, an AP transmits data with the user who occupies the channel for the shortest time, ensuring that each user can equally occupy the wireless channels. The data packets of high-speed users are transmitted quickly, which is not affected by the data transmission time of low-speed users. This improves the overall user experience.

After WMM is enabled on the device and terminals, user packets are scheduled based on different types (service types include VI, VO, BE, and BK). For example, voice packets are scheduled only with other voice packets, and video packets are scheduled only with other video packets.

Precautions

If the packets of multiple users are of different types, airtime fair scheduling is not performed. For example, two users perform packet transmission: one transmits voice packets and the other transmits video packets. In this case, airtime fair scheduling is not performed for the two users.

When the command is executed, the system displays the message "Warning: This action may cause service interruption. Continue?[Y/N]", asking you whether you want to continue.

The airtime fair scheduling function is supported by the following models (enabled by default and cannot be configured using commands):

- AirEngine X760 series APs
- AirEngine X761 series APs

- AirEngine X762 series APs
- AirEngine X771 series APs
- AirEngine series central APs and RUs
- AirEngine 9700D-S (including matching ORUs)

Example

Enable airtime fair scheduling in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] airtime-fair-schedule enable
```

11.7.3 app-share remark

Function

The **app-share remark** command sets a priority for Lync desktop sharing packets.

The **undo app-share remark** command deletes the priority of Lync desktop sharing packets.

By default, the priority of Lync desktop sharing packets is not set.

Format

app-share remark { **8021p** *8021p-value* | **dscp** { *dscp-value* | *dscp-name* } | **local-precedence** { *local-precedence-value* | *local-precedence-name* } }

undo app-share remark { **8021p** | **dscp** | **local-precedence** }

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
dscp { *dscp-value* | *dscp-name* }	Specifies the DSCP priority.	The value is a Diff-Serv code that is an integer ranging from 0 to 63, or a DSCP service type that can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values of service types are as follows: • af11: 10 • af12: 12 • af13: 14 • af21: 18 • af22: 20 • af23: 22 • af31: 26 • af32: 28 • af33: 30 • af41: 34 • af42: 36 • af43: 38 • cs1: 8 • cs2: 16 • cs3: 24 • cs4: 32 • cs5: 40 • cs6: 48 • cs7: 56 • default: 0 • ef: 46

Parameter	Description	Value
local-precedence { *local-precedence-value* | *local-precedence-name* }	Specifies the local priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. Or, the value is a service type that can be af1, af2, af3, af4, be, cs6, cs7, or ef. The values of service types are as follows: • af1: 1 • af2: 2 • af3: 3 • af4: 4 • be: 0 • cs6: 6 • cs7: 7 • ef: 5

Views

UCC profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. You can run the **app-share remark** command to change the priority of Lync desktop sharing packets.

Precautions

The 802.1p priority and local priority cannot be set for the Lync desktop sharing packets of one Lync session.

If you run the **app-share remark** command in the same UCC profile view multiple times to set the 802.1p priority, DSCP priority, or local priority of Lync desktop sharing packets, only the latest configuration takes effect.

Example

Set the DSCP priority of Lync desktop sharing packets to 1 in the UCC profile **test**.


```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] app-share remark dscp 1
```

11.7.4 display references traffic-profile

Function

The **display references traffic-profile** command displays reference information about a traffic profile.

Format

display references traffic-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified traffic profile.	The traffic profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the VAP profiles by which a specified traffic profile is referenced.

Example

Display reference information about the traffic profile **p1**.

```
<HUAWEI> display references traffic-profile name p1
-------------------------------------------------------
Reference type     Reference name
-------------------------------------------------------
VAP profile        default
VAP profile        wlan-vap
VAP profile        exam
VAP profile        test
VAP profile        wlan-vap1
VAP profile        example
VAP profile        2
-------------------------------------------------------
Total: 7
```


Table 11-165 Description of the **display references traffic-profile** command output

Item	Description
Reference type	Type of the profile that references a traffic profile.
Reference name	Name of the profile that references a traffic profile.

11.7.5 display service-experience-analysis monitor-list

Function

The **display service-experience-analysis monitor-list** command displays information about applications monitored based on SEA.

Format

display service-experience-analysis monitor-list [**sta-mac** *sta-mac-address*]

Parameters

Parameter	Description	Value
sta-mac *sta-mac-address*	Displays information about SEA-monitored applications on the STA with a specified MAC address.	The STA's MAC address must exist.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to check information about applications monitored based on SEA, including the STA's MAC address, AP with which the STA is associated, and 5-tuple information in the flow table.

Example

Display information about applications monitored based on SEA.


```
<HUAWEI> display service-experience-analysis monitor-list
-------------------------------------------------------------------------------------------------------------
STA MAC         AP ID AP name Radio ID Protocol Source IP/Port Destination IP/Port
-------------------------------------------------------------------------------------------------------------
1000-0000-0001  1     AP1     1        23       1.1.1.1/100    2.2.2.2/2000
-------------------------------------------------------------------------------------------------------------
Total: 1
```

Table 11-166 Description of the **display service-experience-analysis monitor-list** command output

Item	Description
STA MAC	MAC address of a STA.
AP ID	ID of the AP with which a STA is associated.
AP name	Name of the AP with which a STA is associated.
Radio ID	Radio ID of the AP with which a STA is associated.
Protocol	IP protocol number.
Source IP/Port	Source IP address and source port number.
Destination IP/Port	Destination IP address and destination port number.

11.7.6 display traffic-profile

Function

The **display traffic-profile** command displays configuration information about traffic profiles.

Format

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

Parameters

Parameter	Description	Value
all	Displays configuration information about all traffic profiles.	-

Parameter	Description	Value
name *profile-name*	Displays configuration information about a specified traffic profile.	The value is a string of 1 to 35 characters without spaces and question marks (?). It cannot begin or end with a double quotation mark (").

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the default configurations of a new traffic profile or configurations of an existing traffic profile.

Example

Display configuration information about a traffic profile that maps the trusted user priority from 802.11 packets to tunnel packets when packets are sent from an AP to the AC.

```
<HUAWEI> display traffic-profile name p1
-------------------------------------------------------------------------------------------------
Profile ID                                  : 0
User isolate mode                           : disable
Rate limit client up(Kbps)                  : 4294967295
Rate limit client up(Kbps) with time-range  : -
Rate limit client down(Kbps)                : 4294967295
Rate limit client down(Kbps) with time-range : -
Rate limit VAP up(Kbps)                     : 4294967295
Rate limit VAP down(Kbps)                   : 4294967295
Rate limit client dynamic switch            : enable
Rate limit client dynamic(Mbps)             : 16
Traffic optimize ARP proxy                  : disable
Traffic optimize ND proxy                   : disable
Traffic optimize ARP unicast send           : enable
Traffic optimize ND unicast send            : enable
Traffic optimize DHCP unicast send          : enable
Traffic optimize mDNS unicast send          : enable
Traffic optimize multicast send deny        : disable
Traffic optimize mdns forward               : enable
Traffic optimize TCP adjust MSS(bytes)      : -
Traffic optimize bcmc unicast send mismatch action : drop
MLD snooping                                : disable
IGMP snooping                               : disable
IGMP snooping report suppress               : disable
Spectralink voice priority                  : disable
Priority map upstream trust                 : 8021e
IGMP snooping max bandwidth(kbps)           : -
```



```
IGMP snooping max user                          : -
Traffic optimize sta bridge forward             : enable
Traffic optimize broadcast suppression(pps)     : -
Traffic optimize multicast suppression(pps)     : -
Traffic optimize unicast suppression(pps)       : -
Traffic optimize multicast to unicast           : disable
  Dynamic adaptive                              : enable
Priority map tunnel upstream trust              : 8021e
CAPWAP priority upstream map mode  : 802.11e map DSCP
                                0 map 0
                                1 map 8
                                2 map 16
                                3 map 24
                                4 map 32
                                5 map 40
                                6 map 48
                                7 map 56
CAPWAP priority upstream map mode  : 802.11e map 802.1p
                                0 map 0
                                1 map 1
                                2 map 2
                                3 map 3
                                4 map 4
                                5 map 5
                                6 map 6
                                7 map 7
Priority map downstream trust                   : DSCP
WMM priority downstream map mode   : DSCP map 802.11e
                                0-7 map 0
                                8-15 map 1
                                16-23 map 2
                                24-31 map 3
                                32-39 map 4
                                40-47 map 5
                                48-55 map 6
                                56-63 map 7
WMM priority downstream map mode   : 802.1p map 802.11e
                                0 map 0
                                1 map 1
                                2 map 2
                                3 map 3
                                4 map 4
                                5 map 5
                                6 map 6
                                7 map 7
-------------------------------------------------------------------------------
Traffic Type                    Direction  AppliedRecord
-------------------------------------------------------------------------------
traffic-filter                  inbound    IPv4 ACL 3001 & L2 ACL 4001
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Traffic Type                    Direction  RemarkType  RemarkValue  AppliedRecord
-------------------------------------------------------------------------------
traffic-remark                  inbound    802.11e     0            IPv4 ACL 3001
-------------------------------------------------------------------------------
Wlan-slice high-reliability traffic filter info:
AppliedRecord: IPv4 ACL 3001
```

Table 11-167 Description of the **display traffic-profile** command output

Item	Description
Profile ID	Traffic profile ID.

Item	Description
Priority map downstream trust	Mapping from the 802.1p or DSCP priority of 802.3 packets to the 802.11 user priority when 802.3 packets are sent to an AP from upper-layer devices. To configure this parameter, run the **priority-map downstream trust** command.
User isolate mode	Whether user isolation is enabled. To configure this parameter, run the **user-isolate (traffic profile view)** command.
Rate limit client up(Kbps)	Upstream rate limit configured for STAs. To configure this parameter, run the **rate-limit** command.
Rate limit client up(Kbps) with time-range	Upstream rate limit configured for STAs in a specified time range. To configure this parameter, run the **rate-limit client time-range** command.
Rate limit client down(Kbps)	Downstream rate limit configured for STAs. To configure this parameter, run the **rate-limit** command.
Rate limit client down(Kbps) with time-range	Downstream rate limit configured for STAs in a specified time range. To configure this parameter, run the **rate-limit client time-range** command.
Rate limit VAP up(Kbps)	Upstream rate limit configured for a VAP. To configure this parameter, run the **rate-limit** command.
Rate limit VAP down(Kbps)	Downstream rate limit configured for a VAP. To configure this parameter, run the **rate-limit** command.

Item	Description
Rate limit client dynamic switch	Whether dynamic rate limiting is enabled for a single STA on a VAP. To configure this parameter, run the **rate-limit client dynamic disable** command.
Rate limit client dynamic(Mbps)	Dynamic rate limit threshold for a single STA on a VAP. To configure this parameter, run the **rate-limit client dynamic** command.
Traffic optimize ARP proxy	Whether proxy ARP is enabled for STAs. To configure this parameter, run the **traffic-optimize arp-proxy enable** command.
Traffic optimize ND proxy	Whether ND proxy is enabled for STAs. To configure this parameter, run the **traffic-optimize np-proxy enable** command.
Traffic optimize ARP unicast send	Whether the air interface is enabled to convert broadcast ARP packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send** command.
Traffic optimize ND unicast send	Whether the air interface is enabled to convert multicast ND packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send** command.
Traffic optimize DHCP unicast send	Whether the air interface is enabled to convert broadcast DHCP packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send** command.
Traffic optimize mDNS unicast send	Whether the air interface is enabled to convert broadcast mDNS packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send** command.

Item	Description
Traffic optimize multicast send deny	Whether the air interface is disabled from forwarding multicast packets. To configure this parameter, run the **traffic-optimize bcmc deny all** command.
Traffic optimize mdns forward	Whether the air interface allows mDNS packets to pass through. • enable: The function of denying multicast packets on the air interface is disabled, or this function is enabled but mDNS packets are excluded. • disable: The air interface is disabled from forwarding multicast packets and does not allow mDNS packets to pass through. To configure this parameter, run the **traffic-optimize bcmc deny all** command.
Traffic optimize sta bridge forward	Whether the air interface is configured to deny packets destined for bridge STAs. To configure this parameter, run the **traffic-optimize sta-bridge-forward disable** command.
Traffic optimize bcmc unicast send mismatch action	Action to be taken when the air interface fails to convert broadcast or multicast protocol packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send mismatch-action drop** command.
MLD snooping	Whether MLD snooping is enabled. To configure this parameter, run the **mld-snooping enable (traffic profile view)** command.
IGMP snooping	Whether IGMP snooping is enabled. To configure this parameter, run the **igmp-snooping enable (traffic profile view)** command.

Item	Description
Spectralink voice priority	Whether SVP voice traffic optimization is enabled. To configure this parameter, run the **svp-voice enable** command.
IGMP snooping report suppress	IGMP message suppression time. To configure this parameter, run the **igmp-snooping report-suppress (traffic profile view)** command.
IGMP snooping max bandwidth(kbps)	Maximum multicast bandwidth of a VAP. To configure this parameter, run the **igmp-snooping max-bandwidth (traffic profile view)** command.
IGMP snooping max user	Maximum number of multicast group memberships on a VAP. To configure this parameter, run the **igmp-snooping max-user (traffic profile view)** command.
Traffic optimize broadcast suppression(pps)	Maximum broadcast traffic volume allowed on an interface. To configure this parameter, run the **traffic-optimize broadcast-suppression** command.
Traffic optimize multicast suppression(pps)	Maximum multicast traffic volume allowed on an interface. To configure this parameter, run the **traffic-optimize multicast-suppression** command.
Traffic optimize unicast suppression(pps)	Maximum unicast traffic volume allowed on an interface. To configure this parameter, run the **traffic-optimize unicast-suppression** command.
Traffic optimize multicast to unicast	Whether multicast-to-unicast conversion is enabled. To configure this parameter, run the **traffic-optimize multicast-unicast enable** command.

Item	Description
Dynamic adaptive	Whether adaptive multicast-to-unicast conversion is enabled. To configure this parameter, run the **traffic-optimize multicast-unicast dynamic-adaptive disable** command.
CAPWAP priority upstream map mode	Mapping from the WMM priority of upstream tunnel packets to the DSCP priority.
Priority map tunnel upstream trust	Trusted priority mapping from 802.11 packets to tunnel packets when data packets are sent to the AC from an AP. To configure this parameter, run the **priority-map tunnel-upstream trust** command.
Priority map upstream trust	Trusted priority mapping from 802.11 packets to 802.3 packets when data packets are sent to the AC from an AP. To configure this parameter, run the **priority-map upstream trust** command.
WMM priority downstream map mode	Mapping from the DSCP priority of downstream packets to the WMM priority.
priority upstream map mode	Tunnel upstream mapping when the trusted mapping from 802.11 packets to tunnel packets is DSCP, and data packets are sent to the AC from an AP.
Traffic Type	Traffic control type.
Direction(Traffic Type: traffic-filter)	Direction to which packet filtering is applied. To configure this parameter, run the **traffic-filter (traffic profile view)** command.
AppliedRecord(Traffic Type: traffic-filter)	Application records of ACL-based packet filtering. To configure this parameter, run the **traffic-filter (traffic profile view)** command.

Item	Description
Direction(Traffic Type: traffic-remark)	Direction to which packet priority re-marking is applied. To configure this parameter, run the **traffic-remark (traffic profile view)** command.
RemarkType	Packet priority re-marking type. To configure this parameter, run the **traffic-remark (traffic profile view)** command.
RemarkValue	Re-marked packet priority value. To configure this parameter, run the **traffic-remark (traffic profile view)** command.
AppliedRecord(Traffic Type: traffic-remark)	Application records of ACL-based packet priority re-marking. To configure this parameter, run the **traffic-remark (traffic profile view)** command.
AppliedRecord(Wlan-slice high-reliability traffic filter info)	ACL-based rule records for air interface slicing. To configure this parameter, run the **wlan-slice high-reliability acl** command.

Display configurations of all traffic profiles.

```
<HUAWEI> display traffic-profile all
-------------------------------------------------------
Profile name                    Reference
-------------------------------------------------------
default                          3
1                               1
p1                               0
-------------------------------------------------------
Total: 3
```

Table 11-168 Description of the **display traffic-profile all** command output

Item	Description
Profile name	Profile name. To configure this parameter, run the **traffic-profile (WLAN view)** command.
Reference	Number of times a traffic profile is referenced.

11.7.7 display ucc-profile

Function

The **display ucc-profile** command displays the UCC profile configuration and application.

Format

display ucc-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all UCC profiles.	-
name *profile-name*	Displays information about the specified UCC profile.	The value must be the name of an existing UCC profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a UCC profile is configured, run the **display ucc-profile** command to check the UCC profile configuration and information about the UCC profile bound to a VAP profile.

Example

Display information about all UCC profiles.

```
<HUAWEI> display ucc-profile all
-------------------------------------------------------------
Profile name                Reference
-------------------------------------------------------------
test                        1
-------------------------------------------------------------
```


Table 11-169 Description of the **display ucc-profile all** command output

Item	Description
Profile name	Name of the UCC profile.
Reference	Number of times the UCC profile is bound to the VAP profile.

Display information about the UCC profile **test**.

```
<HUAWEI> display ucc-profile name test
------------------------------------------------------------------------------
Lync app share 802.1p precedence     : -
Lync app share DSCP precedence       : -
Lync app share local precedence      : -
Lync file transfer 802.1p precedence : -
Lync file transfer DSCP precedence   : -
Lync file transfer local precedence  : -
Lync video 802.1p precedence         : 6
Lync video DSCP precedence           : -
Lync video local precedence          : -
Lync voice 802.1p precedence         : -
Lync voice DSCP precedence           : -
Lync voice local precedence          : -
------------------------------------------------------------------------------
```

Table 11-170 Description of the **display ucc-profile name test** command output

Item	Description
Lync app share 802.1p precedence	802.1p priority of Lync desktop sharing packets. To configure the 802.1p priority of Lync desktop sharing packets, run the **app-share remark** command.
Lync app share DSCP precedence	DSCP priority of Lync desktop sharing packets. To configure the DSCP priority of Lync desktop sharing packets, run the **app-share remark** command.
Lync app share local precedence	Local priority of Lync desktop sharing packets. To configure the local priority of Lync desktop sharing packets, run the **app-share remark** command.
Lync file transfer 802.1p precedence	802.1p priority of Lync file transfer packets. To configure the 802.1p priority of Lync file transfer packets, run the **file-transfer remark** command.

Item	Description
Lync file transfer DSCP precedence	DSCP priority of Lync file transfer packets. To configure the DSCP priority of Lync file transfer packets, run the **file-transfer remark** command.
Lync file transfer local precedence	Local priority of Lync file transfer packets. To configure the local priority of Lync file transfer packets, run the **file-transfer remark** command.
Lync video 802.1p precedence	802.1p priority of Lync video packets. To configure the 802.1p priority of Lync video packets, run the **video remark** command.
Lync video DSCP precedence	DSCP priority of Lync video packets. To configure the DSCP priority of Lync video packets, run the **video remark** command.
Lync video local precedence	Local priority of Lync video packets. To configure the local priority of Lync video packets, run the **video remark** command.
Lync voice 802.1p precedence	802.1p priority of Lync voice packets. To configure the 802.1p priority of Lync voice packets, run the **voice remark** command.
Lync voice DSCP precedence	DSCP priority of Lync voice packets. To configure the DSCP priority of Lync voice packets, run the **voice remark** command.
Lync voice local precedence	Local priority of Lync voice packets. To configure the local priority of Lync voice packets, run the **voice remark** command.

11.7.8 file-transfer remark

Function

The **file-transfer remark** command sets a priority for Lync file transfer packets.

The **undo file-transfer remark** command deletes the priority of Lync file transfer packets.

By default, the priority of Lync file transfer packets is not set.

Format

file-transfer remark { **8021p** *8021p-value* | **dscp** { *dscp-value* | *dscp-name* } | **local-precedence** { *local-precedence-value* | *local-precedence-name* } }

undo file-transfer remark { **8021p** | **dscp** | **local-precedence** }

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
dscp { *dscp-value* | *dscp-name* }	Specifies the DSCP priority.	The value is a Diff-Serv code that is an integer ranging from 0 to 63, or a DSCP service type that can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values of service types are as follows: • af11: 10 • af12: 12 • af13: 14 • af21: 18 • af22: 20 • af23: 22 • af31: 26 • af32: 28 • af33: 30 • af41: 34 • af42: 36 • af43: 38 • cs1: 8 • cs2: 16 • cs3: 24 • cs4: 32 • cs5: 40 • cs6: 48 • cs7: 56 • default: 0 • ef: 46

Parameter	Description	Value
local-precedence { *local-precedence-value* | *local-precedence-name* }	Specifies the local priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. Or, the value is a service type that can be af1, af2, af3, af4, be, cs6, cs7, or ef. The values of service types are as follows: • af1: 1 • af2: 2 • af3: 3 • af4: 4 • be: 0 • cs6: 6 • cs7: 7 • ef: 5

Views

UCC profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. You can run the **file-transfer remark** command to change the priority of Lync file transfer packets.

Precautions

The 802.1p priority and local priority cannot be set for the Lync file transfer packets of one Lync session.

If you run the **file-transfer remark** command in the same UCC profile view multiple times to set the 802.1p priority, DSCP priority, or local priority of Lync file transfer packets, only the latest configuration takes effect.

Example

Set the DSCP priority of Lync file transfer packets to 1 in the UCC profile **test**.


```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] file-transfer remark dscp 1
```

11.7.9 game-turbo disable

Function

The **game-turbo disable** command disables the game-turbo function.

The **undo game-turbo disable** command enables the game-turbo function.

By default, the game-turbo function is enabled.

NOTE

The game turbo function is not supported by the following models:

- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W

Format

game-turbo disable

undo game-turbo disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you are playing online games through a WLAN, a network latency may easily lead to skill out-of-control or slow response to actions, deteriorating user experience. In this case, you can enable the game-turbo function to optimize game traffic and reduce the game latency.

Currently, the game-turbo function is available for the following mobile games: *Game for Peace*, *Arena of Valor*, and *World of Tanks Blitz*.

Precautions

Before enabling the game-turbo function, enable the DFI function for application identification.

Example

Enable the game-turbo function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name p1
[HUAWEI-wlan-ssid-prof-p1] undo game-turbo disable
```

11.7.10 lync acl

Function

The **lync acl** command configures the switch to use an ACL to filter packets sent by the Lync server.

The **undo lync acl** command cancels the configuration.

By default, the switch does not use any ACL to filter packets sent by the Lync server.

Format

lync acl *acl-number*

undo lync acl

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL. The basic or advanced ACL must have been created.	The value is an integer. • A basic ACL ranges from 2000 to 2999. • An advanced ACL ranges from 3000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch communicates with the Lync server, to prevent the switch against many packets sent by bogus Lync servers, run the **lync acl** command to configure the switch to use an ACL to filter packets sent by the Lync server.

Prerequisites

A basic or advanced ACL has been created and rules have been configured.

Example

Configure ACL 2001 to allow packets that carry the source address of 192.168.32.1 and are sent by the Lync server.

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.32.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] lync acl 2001
```

11.7.11 lync listener

Function

The **lync listener** command configures the switch to communicate with the Lync server and specifies the port number.

The **undo lync listener** command cancels the configuration.

By default, the switch is not configured to communicate with the Lync server and the port number is not specified.

Format

lync listener { **http-port** *port-num* | **https-port** *port-num* **ssl-policy** *ssl-policy* }

undo lync listener

Parameters

Parameter	Description	Value
http-port *port-num*	Specifies the port number of the HTTP service.	The value is an integer that ranges from 1025 to 55535.
https-port *port-num*	Specifies the port number of the HTTPS service.	The value is an integer that ranges from 1025 to 55535.
ssl-policy *ssl-policy*	Specifies the SSL policy to be bound. The SSL policy must be a server SSL policy.	The value must be the name of an existing SSL policy.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. To ensure normal running of Lync software, configure the switch to communicate with the Lync server.

Precautions

To prevent the impact on the exchange with the Lync server, you are advised to use the port number that is not in use. You can run the **display ip socket register-port** command to check used port numbers.

Example

Configure the switch to communicate with the Lync server and specify HTTP port 2000.

```
<HUAWEI> system-view
[HUAWEI] lync listener http-port 2000
```

11.7.12 multimedia-air-optimize congestion-control tcp-window-tuning disable

Function

The **multimedia-air-optimize congestion-control tcp-window-tuning disable** command disables the TCP window adjustment function for voice and video services.

The **undo multimedia-air-optimize congestion-control tcp-window-tuning disable** command enables the TCP window adjustment function for voice and video services.

By default, the TCP window adjustment function for voice and video services is enabled.

NOTE

The intelligent multimedia scheduling algorithm is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W)
- AirEngine 9700D-S (including matching ORUs)

Format

multimedia-air-optimize congestion-control tcp-window-tuning disable

undo multimedia-air-optimize congestion-control tcp-window-tuning disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA has heavy-traffic services of the AC_BE or AC_BK type in the uplink, packets are frequently sent, and the duration of a single packet transmission is long, the delay of key services in the downlink of the AP is significantly increased. If key downlink services are affected, the system considers performing congestion control on heavy-traffic services of the AC_BE or AC_BK type. The **multimedia-air-optimize congestion-control tcp-window-tuning disable** command is involved for AP uplink congestion control. After the **undo multimedia-air-optimize congestion-control tcp-window-tuning disable** command is executed, the TCP window adjustment function is enabled for voice and video services. If the delay of voice or video services reaches the threshold and the packet transmission duration of heavy-traffic TCP background services in the uplink reaches the threshold within the unit time (1s), the receiver window (RWND) in TCP ACK packets can be dynamically adjusted. This process takes about 5s to 10s. After the adjustment, the uplink data volume sent by STAs is reduced, thereby ensuring user experience of voice and video services.

Prerequisites

The intelligent multimedia scheduling algorithm has been enabled using the **undo multimedia-air-optimize disable** command.

Example

Enable the TCP window adjustment function for voice and video services.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] undo multimedia-air-optimize disable
[HUAWEI-wlan-rrm-prof-p1] undo multimedia-air-optimize congestion-control tcp-window-tuning disable
```

11.7.13 multimedia-air-optimize downlink-delay-guarantee

Function

The **multimedia-air-optimize downlink-delay-guarantee** command configures the guaranteed delay for services of different categories.

The **undo multimedia-air-optimize downlink-delay-guarantee** command restores the default guaranteed delay for services of different categories.

The default guaranteed delay for services of different categories is **medium**.

NOTE

The intelligent multimedia scheduling algorithm is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W)
- AirEngine 9700D-S (including matching ORUs)

Format

multimedia-air-optimize downlink-delay-guarantee { **voice** | **video** | **best-effort** | **background** } { **low** | **medium** | **high** | **off** }

undo multimedia-air-optimize downlink-delay-guarantee

Parameters

Parameter	Description	Value
voice	Specifies voice (AC_VO) packets.	-
video	Specifies video (AC_VI) packets.	-
best-effort	Specifies best-effort (AC_BE) packets.	-
background	Specifies background (AC_BK) packets.	-
low	Sets the guaranteed delay for the service of a specified category to **low**. For specific values, see **Table 11-171**.	-
medium	Sets the guaranteed delay for the service of a specified category to **medium**. For specific values, see **Table 11-171**.	-
high	Sets the guaranteed delay for the service of a specified category to **high**. For specific values, see **Table 11-171**.	-
off	Specifies no delay guarantee for the service of a specified category.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If users have requirements for the delay of voice, best-effort, background, and video services on the air interface, run the **multimedia-air-optimize downlink-delay-guarantee** command to configure the guaranteed delay for voice and video services. With this configuration, the system monitors the delay of services on the air interface in real time. When detecting the delay exceeding the guaranteed delay, the system triggers delay optimization for the corresponding service to ensure that the delay after optimization does not exceed the guaranteed delay.

Table 11-171 Delay guarantee for services

Parameter	Video (UP: 4)	Video (UP: 5)	Voice	Best-Effort	Background
low	Delay < 300 ms	Delay < 100 ms	Delay < 50 ms	Delay < 400 ms	Delay < 500 ms
medium	Delay < 200 ms	Delay < 50 ms	Delay < 20 ms	Delay < 300 ms	Delay < 400 ms
high	Delay < 100 ms	Delay < 20 ms	Delay < 5 ms	Delay < 200 ms	Delay < 300 ms
off	No delay guarantee	No delay guarantee	No delay guarantee	No delay guarantee	No delay guarantee

- UP 4: video applications that support caching, such as online network video and live streaming
- UP 5: video applications that do not support caching, such as network videoconferencing

Prerequisites

The intelligent multimedia scheduling algorithm has been enabled using the **undo multimedia-air-optimize disable** command.

Example

Set the guaranteed delay for video services to **low** and that for voice services to **high**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] undo multimedia-air-optimize disable
[HUAWEI-wlan-rrm-prof-p1] multimedia-air-optimize downlink-delay-guarantee video low
[HUAWEI-wlan-rrm-prof-p1] multimedia-air-optimize downlink-delay-guarantee voice high
```

11.7.14 multimedia-air-optimize disable

Function

The **multimedia-air-optimize disable** command disables the intelligent multimedia scheduling algorithm.

The **undo multimedia-air-optimize disable** command enables the intelligent multimedia scheduling algorithm.

By default, the intelligent multimedia scheduling algorithm is enabled.

NOTE

The intelligent multimedia scheduling algorithm is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W)
- AirEngine 9700D-S (including matching ORUs)

Format

multimedia-air-optimize disable

undo multimedia-air-optimize disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the intelligent multimedia scheduling algorithm is enabled, the system optimizes the air interface traffic in the following aspects:

- Delay guarantee for downlink VI/VO/BE/BK services on an AP

  The system periodically calculates the air interface delay of downlink VI/VO/BE/BK services. When detecting that the current delay exceeds the configured guaranteed delay, the system triggers service delay optimization. The guaranteed delay for VI/VO/BE/BK services is configured using the **multimedia-air-optimize downlink-delay-guarantee** command. After delay optimization for services is complete, the system tries its best to ensure that the service delay does not exceed the guaranteed delay. In addition, the system restricts the VI/VO/BE/BK services of low-speed STAs. Low-speed STAs typically have low transmission efficiency and occupy air interface resources for a long time, increasing the overall delay of VI/VO/BE/BK services. Therefore, the transmission opportunity for such STAs needs to be reduced.
- Delay guarantee for uplink services on an AP

  The system periodically calculates the air interface delay of uplink services (mainly voice and video services, with a user priority of 5 or higher). When detecting that the current delay exceeds the guaranteed delay, the system

triggers service delay optimization. The delay guarantee function for uplink services on an AP can be enabled by using the **undo multimedia-air-optimize uplink-delay-guarantee disable** command. After delay optimization for services is complete, the system tries its best to ensure that the service delay does not exceed the guaranteed delay. In addition, the system restricts the uplink services of low-speed STAs. Low-speed STAs typically have low transmission efficiency and occupy air interface resources for a long time, increasing the overall delay of uplink services. Therefore, the transmission opportunity for such STAs needs to be reduced.

- Preferential scheduling for downlink VI/VO services on an AP

  During software scheduling, VI/VO services are preferentially scheduled. That is, each time the scheduler queries queue information, if the total packet sending time of the current VI/VO queue does not exceed the threshold, the services in the video/voice queue are preferentially scheduled. The threshold is calculated based on the slicing ratio for voice and video services configured using the **multimedia-air-optimize downlink-slice-ratio** command.

- Uplink congestion control for an AP

  When a STA has heavy-traffic services of the AC_BE or AC_BK type in the uplink, packets are frequently sent, and the duration of a single packet transmission is long, the delay of key services in the downlink of the AP is significantly increased. If key downlink services are affected, the system considers performing congestion control on heavy-traffic services of the AC_BE or AC_BK type. The **multimedia-air-optimize congestion-control tcp-window-tuning disable** command is involved for AP uplink congestion control. After the **undo multimedia-air-optimize congestion-control tcp-window-tuning disable** command is executed, the TCP window adjustment function is enabled for voice and video services. If the delay of voice or video services reaches the threshold and the packet transmission duration of heavy-traffic TCP background services in the uplink reaches the threshold within the unit time (1s), the receiver window (RWND) in TCP ACK packets can be dynamically adjusted. This process takes about 5s to 10s. After the adjustment, the uplink data volume sent by STAs is reduced, thereby ensuring user experience of voice and video services.

- WMM parameter adjustment based on the number of access STAs

  After the intelligent multimedia scheduling algorithm is enabled, the system dynamically adjusts WMM parameters based on the number of access users, improving voice and video service experience.

  The number of voice/video users is identified based on the user packet threshold configured using the **multimedia-air-optimize threshold** command. If the number of voice or video packets sent by a user in the internal statistics queue of a radio within the unit time (1 second) exceeds the threshold, the user is considered a voice or video user.

Ensure that the WMM function is enabled (default). To enable the WMM function, run the **undo wmm disable**.

Precautions

After the **undo multimedia-air-optimize disable** command is executed, the **wmm edca-ap** and **wmm edca-client (SSID profile view)** commands do not take effect.

Example

Enable the intelligent multimedia scheduling algorithm in the RRM profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] undo multimedia-air-optimize disable
```

11.7.15 multimedia-air-optimize threshold

Function

The **multimedia-air-optimize threshold** command sets a user packet threshold in the intelligent multimedia scheduling algorithm.

The **undo multimedia-air-optimize threshold** command restores the default user packet threshold.

By default, the video user packet threshold is 100 pps, and the default voice user packet threshold is 30 pps.

NOTE

The intelligent multimedia scheduling algorithm is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W)
- AirEngine 9700D-S (including matching ORUs)

Format

multimedia-air-optimize threshold { **video** *video* | **voice** *voice* } *

undo multimedia-air-optimize threshold

Parameters

Parameter	Description	Value
video *video*	Specifies the video packet threshold.	The value is an integer that ranges from 10 to 1000.
voice *voice*	Specifies the voice packet threshold.	The value is an integer that ranges from 10 to 1000.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the intelligent multimedia scheduling algorithm is enabled, the system uses algorithms to dynamically adjust EDCA parameters and ACK policies based on the number of access users, improving user experience of voice and video applications.

Prerequisites

The intelligent multimedia scheduling algorithm has been enabled using the **undo multimedia-air-optimize disable** command.

Example

Set the user packet thresholds for voice and video services in the intelligent multimedia scheduling algorithm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] multimedia-air-optimize threshold video 100 voice 30
```

11.7.16 priority-map downstream dot1p

Function

The **priority-map downstream dot1p** command configures mapping from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets when packets are sent to an AP from upper-layer devices.

The **undo priority-map downstream dot1p** command restores the default mapping from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets when packets are sent to an AP from upper-layer devices.

By default, 802.1p priority 0 of 802.3 packets maps to user priority 0 of 802.11 packets, 802.1p priority 1 to user priority 1, and similarly, 802.1p priority 7 to user priority 7.

Format

priority-map downstream dot1p { *dot1p-value1* [**to** *dot1p-value2*] } &<1-7> **dot11e** *dot11e-value*

undo priority-map downstream dot1p

Parameters

Parameter	Description	Value
dot1p *dot1p-value1*	Specifies the 802.1p priority in an 802.3 packet.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
to *dot1p-value2*	Specifies the 802.1p priority in an 802.3 packet.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. *dot1p-value2* must be greater than *dot1p-value1*.
dot11e *dot11e-value*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 data packets use different fields to identify their priorities. 802.11 packets sent from a WMM-capable STA carry the user priority (also called the User Priority field), and VLAN tagged-802.3 packets transmitted on the Ethernet contain 802.1p priorities (also called the CoS field). When data packets are forwarded from the AC or upper-layer network to an AP, the AP needs to convert the 802.3 packets to 802.11 packets and map the 802.1p priority carried in the 802.3 packet header to the user priority of 802.11 packets. You can use the **priority-map downstream dot1p** command to configure mapping from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets.

Example

Configure the mapping from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets in traffic profile **p1**.

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



```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map downstream dot1p 0 dot11e 2
```

11.7.17 priority-map downstream dscp

Function

The **priority-map downstream dscp** command configures mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets when packets are sent to an AP from upper-layer devices.

The **undo priority-map downstream dscp** command restores the default mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets when packets are sent to an AP from upper-layer devices.

Table 11-172 describes the default mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets.

Table 11-172 Default mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets

DSCP	UP
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Format

priority-map downstream dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot11e** *dot11e-value*

undo priority-map downstream dscp

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority. *dscp-value2* must be greater than *dscp-value1*.
dot11e *dot11e-value*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 data packets use different fields to identify their priorities. 802.11 packets sent from a WMM-capable STA carry the user priority (also called the User Priority field), and IP packets transmitted on an Ethernet carry the DSCP priority (also called the ToS field). When data packets are forwarded from the central AP or upper-layer network to an RU, the RU needs to convert the 802.3 packets to 802.11 packets and map the ToS field in the IP packet header to the UP field of 802.11 packets. You can use the **priority-map downstream dscp** command to configure mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets.

Example

Configure mapping from the DSCP priority of 802.3 packets in traffic profile **p1** to the user priority of 802.11 packets.

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



```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map downstream dscp 0 to 6 dot11e 0
```

11.7.18 priority-map downstream trust

Function

The **priority-map downstream trust** command configures a trusted priority type used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

The **undo priority-map downstream trust** command restores the default trusted priority type used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

By default, the DSCP priority is used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

Format

priority-map downstream trust { **dot1p** | **dscp** }

undo priority-map downstream trust

Parameters

Parameter	Description	Value
dot1p	Specifies the 802.1p priority as the trusted priority type used in mapping from 802.3 packets to 802.11 packets.	-
dscp	Specifies the DSCP priority as the trusted priority type used in mapping from 802.3 packets to 802.11 packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 data packets use different fields to identify their priorities. 802.11 packets sent from a WMM-capable STA carry the user priority (also called the User Priority field). On a wired network, VLAN packets carry the 802.1p priority and IP packets carry the DSCP priority. When data packets are forwarded from the AC or other upper-layer devices to an AP, the packets must be converted from 802.3 packets to 802.11 packets.

You can run the **priority-map downstream trust** command to configure a trusted priority type used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

Example

In traffic profile **p1**, configure the 802.1p priority as the trusted priority type used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map downstream trust dot1p
```

11.7.19 priority-map tunnel-upstream dot11e dscp

Function

The **priority-map tunnel-upstream dot11e dscp** command configures mapping from the user priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream dot11e dscp** command restores the default mapping from the user priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

Table 11-173 describes the default mapping from the user priority of 802.11 packets to the DSCP priority of tunnel packets.

NOTE

The CAPWAP header refers to the tunnel header.

Table 11-173 Default mapping from user priorities of 802.11 packets to DSCP priorities in CAPWAP headers

User Priority of 802.11 Packets	DSCP Priority in the CAPWAP Header
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Format

priority-map tunnel-upstream dot11e { *dot11e-value1* [**to** *dot11e-value2*] } &<1-7> **dscp** *dscp-value*

undo priority-map tunnel-upstream dot11e to dscp

Parameters

Parameter	Description	Value
dot11e *dot11e-value1*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
to *dot11e-value2*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. *dot11e-value2* must be greater than *dot11e-value1*.
dscp *dscp-value*	Specifies the DSCP priority of tunnel packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry the user priority (Layer 2) or DSCP priority (Layer 3), and tunnel packets carry the 802.1p priority (Layer 2) or tunnel DSCP priority (Layer 3). 802.11 packets sent to the AC from an AP must be converted into tunnel packets.

You can run the **priority-map tunnel-upstream dot11e dscp** command to configure mapping from the user priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, configure mapping from user priority 6 of 802.11 packets to DSCP priority 1 of tunnel packets when packets are sent to the AC from an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream dot11e 6 dscp 1
```

11.7.20 priority-map tunnel-upstream dot11e dot1p

Function

The **priority-map tunnel-upstream dot11e dot1p** command configures mapping from user priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream dot11e dot1p** command restores the default mapping from user priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

By default, user priority 0 of 802.11 packets maps to 802.1p priority 0 of tunnel packets, user priority 1 to 802.1p priority 1, and similarly, user priority 7 to 802.1p priority 7.

Format

priority-map tunnel-upstream dot11e { *dot11e-value1* [**to** *dot11e-value2*] } &<1-7> **dot1p** *dot1p-value*

undo priority-map tunnel-upstream dot11e to dot1p

Parameters

Parameter	Description	Value
dot11e *dot11e-value1*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
to *dot11e-value2*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. *dot11e-value2* must be greater than *dot11e-value1*.
dot1p *dot1p-value*	Specifies the 802.1p priority of tunnel packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry user priorities (Layer 2 priorities) or DSCP priorities (Layer 3 priorities). Tunnel packets carry 802.1p priorities (Layer 2 priorities) or DSCP priorities (Layer 3 priorities). When data packets are sent from APs to the AC, 802.11 packets need to be converted to tunnel packets.

You can run the **priority-map tunnel-upstream dot11e dot1p** command to configure mapping from user priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, map user priority 6 of 802.11 packets to 802.1p priority 1 of tunnel packets when data is sent from APs to the AC.

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



```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream dot11e 6 dot1p 1
```

11.7.21 priority-map tunnel-upstream dscp dot1p

Function

The **priority-map tunnel-upstream dscp dot1p** command configures mapping from DSCP priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream dscp dot1p** command restores the default mapping from DSCP priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

Table 11-174 describes the default mapping from DSCP priorities of 802.11 packets to 802.1p priorities of tunnel packets.

NOTE

The CAPWAP header refers to the tunnel header.

Table 11-174 Default mapping from DSCP priorities of 802.11 packets to 802.1p priorities of in CAPWAP headers

DSCP Priority of 802.11 Packets	802.1p Priority in the CAPWAP Header
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Format

priority-map tunnel-upstream dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot1p** *dot1p-value*

undo priority-map tunnel-upstream dscp to dot1p

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority. *dscp-value2* must be greater than *dscp-value1*.
dot1p *dot1p-value*	Specifies the 802.1p priority of tunnel packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry user priorities (Layer 2 priorities) or DSCP priorities (Layer 3 priorities). Tunnel packets carry 802.1p priorities (Layer 2 priorities) or DSCP priorities (Layer 3 priorities). When data packets are sent from APs to the AC, 802.11 packets need to be converted to tunnel packets.

You can run the **priority-map tunnel-upstream dscp dot1p** command to configure mapping from DSCP priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, map DSCP priorities 0 to 7 of 802.11 packets to 802.1p priority 1 of tunnel packets when data is sent from APs to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream dscp 0 to 7 dot1p 1
```

11.7.22 priority-map tunnel-upstream dscp tunnel-dscp

Function

The **priority-map tunnel-upstream dscp tunnel-dscp** command configures mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream dscp tunnel-dscp** command restores the default mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

By default, DSCP priority **1** of 802.11 packets maps DSCP priority **1** of tunnel packets, DSCP priority **2** of 802.11 packets maps DSCP priority **2** of tunnel packets, and so on. DSCP priority **63** of 802.11 packets maps DSCP priority **63** of tunnel packets.

Format

priority-map tunnel-upstream dscp { *dscp-value* [**to** *dscp-value1*] } &<1-10> **tunnel-dscp** *dscp-value2*

undo priority-map tunnel-upstream dscp to tunnel-dscp

Parameters

Parameter	Description	Value
dscp *dscp-value*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Parameter	Description	Value
to *dscp-value1*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority. *dscp-value1* must be greater than *dscp-value*.
tunnel-dscp *dscp-value2*	Specifies the DSCP priority of tunnel packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry the user priority (Layer 2) or DSCP priority (Layer 3), and tunnel packets carry the 802.1p priority (Layer 2) or tunnel DSCP priority (Layer 3). 802.11 packets sent to the AC from an AP must be converted into tunnel packets.

You can run the **priority-map tunnel-upstream dscp tunnel-dscp** command to configure mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, configure mapping from DSCP priority 6 of 802.11 packets to DSCP priority 1 of tunnel packets when packets are sent to the AC from an AP.

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



```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream dscp 6 tunnel-dscp 1
```

11.7.23 priority-map tunnel-upstream trust

Function

The **priority-map tunnel-upstream trust** command configures a trusted priority type used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream trust** command restores the default trusted priority type used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

By default, the 802.11e priority is used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

Format

priority-map tunnel-upstream trust { **dot11e** | **dscp** }

undo priority-map tunnel-upstream trust

Parameters

Parameter	Description	Value
dot11e	Specifies the 802.11e priority as the trusted priority type used in mapping from 802.11 packets to tunnel packets.	-
dscp	Specifies the DSCP priority as the trusted priority type used in mapping from 802.11 packets to tunnel packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry the user priority (Layer 2) or DSCP priority (Layer 3), and tunnel packets carry the 802.1p priority (Layer 2) or

tunnel DSCP priority (Layer 3). 802.11 packets sent to the AC from an AP must be converted into tunnel packets.

You can run the **priority-map tunnel-upstream trust** command to configure a trusted priority type used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, configure the DSCP priority as the trusted priority type used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream trust dscp
```

11.7.24 priority-map upstream trust

Function

The **priority-map upstream trust** command configures the priority mapping mode from 802.11 packets to 802.3 packets when packets are sent from an AP to upper-layer devices.

The **undo priority-map upstream trust** command restores the default priority mapping mode from 802.11 packets to 802.3 packets when packets are sent from an AP to upper-layer devices.

By default, the 802.11e priority is mapped from 802.11 packets to 802.3 packets when packets are sent from an AP to upper-layer devices.

Format

priority-map upstream trust { **dot11e** | **dscp** }

undo priority-map upstream trust

Parameters

Parameter	Description	Value
dot11e	Specifies the mapping from the user priority of 802.11 packets to the DSCP and 802.1p priorities of 802.3 packets.	-
dscp	Specifies the DSCP priority mapping from 802.11 packets to 802.3 packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 data packets use different fields to identify their priorities. 802.11 packets sent from a WMM-capable STA carry the user priority (also called the User Priority field), and IP packets transmitted on an Ethernet carry the DSCP priority (also called the ToS field). When data packets are forwarded from an AP to an AC or the upper-layer network, 802.3 packets need to be converted into 802.11 packets. During the conversion, the user priority of 802.11 packets is mapped to the ToS field in the IP packet header.

Currently, the priority mappings are fixed and described in the following table.

Table 11-175 Mapping between the DSCP and 802.1p priorities

DSCP Priority of 802.11 Packets	802.1p Priority of 802.3 Packets
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Table 11-176 Mapping from the user priority to the 802.1p and DSCP priorities

User Priority of 802.11 Packets	DSCP Priority of 802.3 Packets	802.1p Priority of 802.3 Packets
0	0	0
1	8	1
2	16	2
3	24	3
4	32	4

User Priority of 802.11 Packets	DSCP Priority of 802.3 Packets	802.1p Priority of 802.3 Packets
5	40	5
6	48	6
7	56	7

Example

Configure the DSCP priority mapping from 802.11 packets to 802.3 packets in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map upstream trust dscp
```

11.7.25 qos car (SSID profile view)

Function

The **qos car** command configures QoS CAR parameters.

The **undo qos car** command deletes the configured QoS CAR parameters.

By default, no QoS CAR parameters are configured in an SSID profile.

Format

qos car inbound cir *cir-value* [**cbs** *cbs-value* [**pbs** *pbs-value*] | **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]

undo qos car inbound

Parameters

Parameter	Description	Value
inbound	Applies a QoS CAR profile to the inbound direction of an interface.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.

Parameter	Description	Value
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The PIR value must be greater than or equal to the CIR value.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. By default: • If the PIR value is not set, the CBS value is 188 times the CIR value. If the value 188 times the CIR exceeds the maximum value (4294967295) of the CBS, 4294967295 is used. • If the PIR is set, the CBS is 125 times the CIR. If the value 125 times the CIR exceeds the maximum value (4294967295) of the CBS, 4294967295 is used.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. By default, if the PIR is set, the PBS is 125 times the PIR. If the value 125 times the PIR exceeds the maximum value (4294967295) of the PBS, 4294967295 is used.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic policing discards excess traffic to limit incoming and outgoing traffic within a proper range and to protect network resources.

When traffic is transmitted from a high-speed link to a low-speed link, the inbound interface of the low-speed link is prone to severe data loss. The data traffic rate needs to be limited. To solve this problem, configure traffic policing for outgoing traffic on the interface of the high-speed link. The interface then discards the packets whose rate exceeds the traffic policing rate, limiting the outgoing traffic rate in a proper range. You can also configure traffic policing for incoming traffic on the interface of the low-speed link. The interface then discards the received packets whose rate exceeds the traffic policing rate.

The packet color is determined by parameters **cbs** *cbs-value* and **pbs** *pbs-value* of this command.

- When the size of a packet is less than the CBS value, the packet is colored green.
- When the size of a packet is greater than or equal to the CBS value but less than the PBS value, the packet is colored yellow.
- When the size of a packet is greater than or equal to the PBS value, the packet is colored red.

QoS CAR parameters can be configured in an SSID profile to implement traffic policing on user traffic on all VAPs to which the user profile is applied. These VAPs share a token bucket, and more VAPs indicate fewer network resources that each VAP can occupy.

Precautions

QoS CAR parameters configured in an SSID profile are valid only when the service data forwarding mode is set to tunnel forwarding. In tunnel forwarding mode, this function does not take effect when Layer 2 STAs associated with the same AP communicate with each other.

When the traffic policing rate is greater than the maximum rate of an interface, traffic policing does not take effect on the interface. Set the value of *cir-value* smaller than the rate of the interface.

When the CBS value is smaller than the number of bytes in a packet, packets of this type are discarded.

To ensure that the device correctly identifies packet colors, you are advised to set the PBS value greater than the CBS value.

When a user is configured as a VIP user, the QoS CAR configured in the SSID profile does not take effect.

Example

Configure traffic policing parameters for incoming packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name p1
[HUAWEI-wlan-ssid-prof-p1] qos car inbound cir 64 cbs 9000 pbs 18000
```


11.7.26 rate-limit

Function

The **rate-limit** command configures the rate limit for upstream and downstream packets of all STAs or each STA on a VAP.

The **undo rate-limit** command restores the default rate limit for upstream and downstream packets of all STAs or each STA on a VAP.

By default, the rate limit for upstream and downstream packets of all STAs on a VAP is 4294967295 kbit/s, and that of each STA is 4294967295 kbit/s.

Format

rate-limit { **client** | **vap** } { **up** | **down** } *rate-value*

undo rate-limit { **client** | **vap** } { **up** | **down** }

Parameters

Parameter	Description	Value
client	Specifies a STA on a VAP.	-
vap	Specifies all STAs on a VAP.	-
up	Specifies the rate limit for upstream packets on a VAP.	-
down	Specifies the rate limit for downstream packets on a VAP.	-
rate-value	Specifies the rate limit of packets.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The value **4294967295** indicates that the rate is not limited.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **rate-limit** command to limit the rate of upstream and downstream packets for all STAs or each STA on a VAP to protect network bandwidth resources.

Precautions

The limited rate does not take effect for STAs that go online before the **rate-limit** command is configured. To make this configuration take effect for a STA, enable the STA to go online again.

The rate limit configured for each STA on a VAP does not take effect for multicast packets.

When the NP fast forwarding function is disabled, neither the **rate-limit vap** nor **rate-limit client** command configuration takes effect for VIP users. When the NP fast forwarding function is enabled, the **rate-limit vap** command configuration takes effect for VIP users, but the **rate-limit client** command configuration does not take effect for VIP users.

Example

Set the rate limit of upstream packets to 4294967295 kbit/s for all STAs on a VAP in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] rate-limit vap up 4294967295
```

11.7.27 rate-limit client dynamic

Function

The **rate-limit client dynamic** command sets the dynamic rate limit threshold for a single STA in a VAP.

The **undo rate-limit client dynamic** command restores the default dynamic rate limit threshold for a single STA in a VAP.

By default, the dynamic rate limit threshold for a single STA in a VAP is 16 Mbit/s.

NOTE

Dynamic rate limiting for STAs is not supported by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs
- AirEngine X762 series APs
- AirEngine X771 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

rate-limit client dynamic *rate-value*

undo rate-limit client dynamic

Parameters

Parameter	Description	Value
rate-value	Specifies the rate limit of packets.	The value is an enumerated value, which can be 8, 16, or 32, in Mbit/s. The default value is 16 Mbit/s.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA downloads or uploads large files on the live network, network access of other STAs may be affected.

After dynamic rate limiting is enabled, the device determines whether to perform three-phase rate limiting for wireless users depending on whether the air interface is congested. This improves network experience of wireless users.

Precautions

If static rate limiting has been enabled, static rate limiting takes precedence over dynamic rate limiting.

When the NP fast forwarding function is disabled, neither the **rate-limit vap** nor **rate-limit client** command configuration takes effect for VIP users. When the NP fast forwarding function is enabled, the **rate-limit vap** command configuration takes effect for VIP users, but the **rate-limit client** command configuration does not take effect for VIP users.

Example

Set the dynamic rate limit threshold for a single STA in a VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] undo rate-limit client dynamic disable
[HUAWEI-wlan-traffic-prof-p1] rate-limit client dynamic 32
```


11.7.28 rate-limit client dynamic disable

Function

The **rate-limit client dynamic disable** command disables dynamic rate limiting for a single STA in a VAP.

The **undo rate-limit client dynamic disable** command enables dynamic rate limiting for a single STA in a VAP.

By default, dynamic rate limiting is enabled for a single STA in a VAP.

NOTE

Dynamic rate limiting for STAs is not supported by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs
- AirEngine X762 series APs
- AirEngine X771 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

rate-limit client dynamic disable

undo rate-limit client dynamic disable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA downloads or uploads large files on the live network, network access of other STAs may be affected.

After dynamic rate limiting is enabled, the device determines whether to perform three-phase rate limiting for wireless users depending on whether the air interface is congested. This improves network experience of wireless users.

Precautions

If static rate limiting has been enabled, static rate limiting takes precedence over dynamic rate limiting.

When the NP fast forwarding function is disabled, neither the **rate-limit vap** nor **rate-limit client** command configuration takes effect for VIP users. When the NP fast forwarding function is enabled, the **rate-limit vap** command configuration takes effect for VIP users, but the **rate-limit client** command configuration does not take effect for VIP users.

Example

Enable dynamic rate limiting for a single STA in a VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] undo rate-limit client dynamic disable
```

11.7.29 rate-limit client time-range

Function

The **rate-limit client time-range** command sets a rate limit for upstream or downstream packets of each STA on a VAP in a specified time range.

The **undo rate-limit client time-range** command restores the default rate limit of upstream or downstream packets of each STA on a VAP in a specified time range.

By default, no rate limit is set for upstream or downstream packets of each STA on a VAP in a specified time range.

Format

rate-limit client { **up** | **down** } *rate-value* **time-range** *time-range-name*

undo rate-limit client { **up** | **down** } **time-range** *time-range-name*

Parameters

Parameter	Description	Value
client	Specifies each STA on a VAP.	-
up	Specifies the rate limit for upstream packets of each STA on a VAP.	-
down	Specifies the rate limit for downstream packets of each STA on a VAP.	-

Parameter	Description	Value
rate-value	Specifies the rate limit of packets.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The value **4294967295** indicates that the packet rate is not limited.
time-range-name	Specifies the name of a time range during which the rate of packets is limited.	The value is a string of 1 to 32 characters and must begin with a letter. To avoid confusion, do not use **all** as the name of a time range.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **rate-limit client time-range** command to set a rate limit for upstream or downstream packets of each STA on a VAP in a specified time range.

Precautions

The limited rate does not take effect for STAs that go online before the **rate-limit** command is configured. To make this configuration take effect for a STA, enable the STA to go online again.

The rate limit configured for each STA on a VAP does not take effect for multicast packets.

When the NP fast forwarding function is disabled, neither the **rate-limit vap** nor **rate-limit client** command configuration takes effect for VIP users. When the NP fast forwarding function is enabled, the **rate-limit vap** command configuration takes effect for VIP users, but the **rate-limit client** command configuration does not take effect for VIP users.

A maximum of eight time range–based rate limiting policies can be configured in the same direction (upstream or downstream). By default, the device has a default

policy (determined by the **rate-limit client** { **up** | **down** } *rate-value* command configuration). A configured time range–based rate limiting policy takes precedence over the default policy. If multiple time range–based rate limiting policies are configured, the minimum rate limit value takes effect.

You need to run the **time-range** command in the system view to configure a time range.

Example

Set the rate limit for upstream packets of each STA on a VAP to 1000 kbit/s in the time range named **time**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] rate-limit client up 1000 time-range time
Warning: The specified time-range does not exist. You can create it later. Continue?[Y/N]y
```

11.7.30 rate-limit dynamic interval

Function

The **rate-limit dynamic interval** command sets the detection interval and threshold for dynamic rate limiting of a single STA on a VAP.

The **undo rate-limit dynamic** command restores the default detection interval and threshold for dynamic rate limiting of a single STA on a VAP.

The default detection interval and threshold for dynamic rate limiting of a single STA on a VAP are 5 and 80%, respectively.

Format

rate-limit dynamic interval *interval* **threshold** *threshold*

undo rate-limit dynamic

Parameters

Parameter	Description	Value
interval	Specifies the detection interval for dynamic rate limiting.	The value is an integer that ranges from 1 to 30.
threshold *threshold*	Specifies the detection threshold for dynamic rate limiting.	The value is an integer that ranges from 1 to 100.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to adjust the time when dynamic rate limiting takes effect.

If the channel utilization is higher than *threshold*% for a consecutive number of times specified by *interval* (that is, a period of time specified by *interval* x 2 seconds), the air interface congestion is determined.

Example

Configure the detection interval and threshold for dynamic rate limiting of a single STA on a VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] rate-limit dynamic interval interval 10 threshold 60
```

11.7.31 svp-voice enable

Function

The **svp-voice enable** command enables the Spectralink Voice Priority (SVP) voice traffic optimization function.

The **undo svp-voice enable** command disables the SVP voice traffic optimization function.

By default, the SVP voice traffic optimization function is disabled.

Format

svp-voice enable

undo svp-voice enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

SpectraLink Voice is a voice protocol defined by Spectralink (a Wi-Fi phone company). To ensure SpectraLink voice transmission quality on WLANs, SpectraLink defines SpectraLink Voice Priority (SVP) to describe the requirements of SpectraLink Voice on WLANs.

On a WLAN with STAs supporting the SpectraLink Voice protocol, you are advised to enable the SVP voice traffic optimization function.

Example

Enable the SVP voice traffic optimization function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] svp-voice enable
```

11.7.32 service-experience-analysis enable

Function

The **service-experience-analysis enable** command enables the service experience analysis (SEA) function.

The **undo service-experience-analysis enable** command disables the service experience analysis (SEA) function.

By default, the SEA function is disabled.

NOTE

This command is not supported by the following models:

- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis enable

undo service-experience-analysis enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the SIP (eSpace) service runs on a WLAN, you can enable the SEA function so that the device reports performance statistics about SIP traffic (such as IP addresses and port numbers of calling and called parties, and call quality data) to iMaster NCE-CampusInsight. In this manner, iMaster NCE-CampusInsight can analyze network performance and locate faults.

Follow-up Procedure

Run the **service-experience-analysis sip-snooping port** command to set the port number for identifying SIP packets.

Example

Enable the SEA function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name example
[HUAWEI-wlan-vap-prof-example] service-experience-analysis enable
```

11.7.33 service-experience-analysis monitor interval

Function

The **service-experience-analysis monitor interval** command configures the sampling interval for SEA-based application monitoring.

The **undo service-experience-analysis monitor interval** command restores the default sampling interval for SEA-based application monitoring.

By default, the sampling interval for SEA-based application monitoring is 10 seconds.

NOTE

This command is not supported by the following models:

- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis monitor interval *interval*

undo service-experience-analysis monitor interval

Parameters

Parameter	Description	Value
interval	Specifies the sampling interval for SEA-based application monitoring.	The value is an integer that ranges from 2 to 30, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure the sampling interval for SEA-based application monitoring.

Example

Set the sampling interval for SEA-based application monitoring to 2 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys
[HUAWEI-wlan-ap-system-prof-apsys] service-experience-analysis monitor interval 2
```

11.7.34 service-experience-analysis monitor application

Function

The **service-experience-analysis monitor application** command configures an application to be monitored based on SEA.

The **undo service-experience-analysis monitor application** command deletes an application monitored based on SEA.

By default, no application is monitored based on SEA.

NOTE

This command is not supported by the following models:

- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis monitor application *appname*

undo service-experience-analysis monitor application *appname*

Parameters

Parameter	Description	Value
appname	Specifies an application to be monitored based on SEA.	Currently, applications that use the TCP and RTP protocols can be monitored based on SEA. RTP-based applications include: • skype_voip • sip • rtp • whatsapp • espace_voip • hangouts • slack_voip • welink_videocall • microsoftteams • webex_voip • xiaoyuyilian • huaweimeeting

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure application-based traffic quality monitoring. After the configuration is complete, the AC delivers the configuration to APs that will monitor the specified application.

Prerequisites

The security engine has been enabled using the **defence engine enable** command.

Precautions

You can configure a maximum of 16 applications to be monitored based on SEA.

For some voice and video applications, if the application control packets use TCP and the data packets use UDP, the device can monitor only the quality of application control packets (TCP).

Among user-defined applications (created using the **user-defined-application** command), SEA can monitor only user-defined TCP applications (specified by the **protocol tcp** parameter) but not user-defined UDP applications (specified by the **protocol udp** parameter).

SEA does not monitor fragmented packets.

Example

Configure an application to be monitored based on SEA.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] service-experience-analysis monitor application WeLink
```

11.7.35 service-experience-analysis monitor ucl-group

Function

The **service-experience-analysis monitor ucl-group** command specifies a UCL group or a "UCL group + application" combination monitored based on SEA.

The **undo service-experience-analysis monitor ucl-group** command deletes a UCL group or a "UCL group + application" combination monitored based on SEA.

By default, no UCL group is monitored based on SEA.

NOTE

This command is not supported by the following models:

- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis monitor ucl-group { *group-index* | **name** *group-name* } [**application** *application-name* & <1-16>]

undo service-experience-analysis monitor ucl-group { *group-index* | **name** *group-name* } [**application** *application-name* &<1-16>]

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The value is an integer that ranges from 1 to 64000.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.

Parameter	Description	Value
application *application-name*	Specifies an application to be monitored based on SEA.	The application must exist. A maximum of 16 applications can be specified.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify a UCL group or a "UCL group + application" combination to be monitored based on SEA.

You can specify a UCL group so that the device can monitor the quality of applications of users in the specified UCL group. You can also specify a "UCL group + application" combination, so that the device can monitor the quality of the specified application of users in the specified UCL group.

Precautions

A maximum of 128 applications, UCL groups, and "UCL group + application" combinations (including 16 applications at most) can be monitored based on SEA.

Example

Specify the application **WeLink** in the UCL group **test** to be monitored based on SEA.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] service-experience-analysis monitor ucl-group test application WeLink
```

11.7.36 service-experience-analysis sip-snooping port

Function

The **service-experience-analysis sip-snooping port** command sets the port number for identifying SIP packets.

The **undo service-experience-analysis sip-snooping port** command restores the default port number for identifying SIP packets.

The default port number for identifying SIP packets is 5060.

NOTE

This command is not supported by the following models:

- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis sip-snooping port *port-number*

undo service-experience-analysis sip-snooping port

Parameters

Parameter	Description	Value
port-number	Specifies the port number for identifying SIP packets.	The value is an integer that ranges from 1 to 65535.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

When the SIP (eSpace) service runs on a WLAN, you can enable the SEA function so that the device reports performance statistics about SIP traffic (such as IP addresses and port numbers of calling and called parties, and call quality data) to iMaster NCE-CampusInsight. In this manner, iMaster NCE-CampusInsight can analyze network performance and locate faults.

You can run this command to configure the port number for identifying SIP packets.

Before specifying the port number for identifying SIP packets, enable the SEA function using the **service-experience-analysis enable** command.

Example

Set the port number for identifying SIP packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name example
[HUAWEI-wlan-vap-prof-example] service-experience-analysis sip-snooping port 5080
```


11.7.37 traffic-filter (traffic profile view)

Function

The **traffic-filter** command configures ACL-based packet filtering in a traffic profile.

The **undo traffic-filter** command cancels the configuration of ACL-based packet filtering in a traffic profile.

By default, ACL-based packet filtering is not configured in a traffic profile.

Format

traffic-filter { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

traffic-filter { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based packet filtering in the inbound direction.	-
outbound	Configures ACL-based packet filtering in the outbound direction.	-
ipv4	Configures ACL-based IPv4 packet filtering.	-
ipv6	Configures ACL-based IPv6 packet filtering.	-
l2	Configures ACL-based Layer 2 packet filtering.	-

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031 and from 6000 to 6031 for an IPv4 ACL, from 3000 to 3031 and 6000 to 6031 for an IPv6 ACL, and from 4000 to 4031 for a Layer 2 ACL. • 3000 to 3031: advanced ACLs • 6000 to 6031: user ACLs • 4000 to 4031: Layer 2 ACLs
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of an ACL.	The value is a string of 1 to 65 case-sensitive characters without spaces and must begin with a letter. The value range of *acl-number* corresponding to *acl-name* is 3000 to 3031, and 6000 to 6031.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a wireless network, administrators want to provide differentiated services for wireless users. The services may include, but are not limited to the following:

- Deny or permit access of specified wireless users to specified LAN devices.
- Deny access of specified wireless users to specified invalid IP addresses.

You can configure ACL-based packet filtering in a traffic profile for providing differentiated services to wireless users based on ACL rules.

When the **traffic-filter** command is configured in the traffic profile view, the device first matches packets against ACLs and then performs the action according to the matched policy.

When multiple **traffic-filter** commands are configured for ACL-based packet filtering in the same direction in the same traffic profile, packets are matched against the next rule in the sequence in which the commands are configured. If packets match a rule, the device executes the specified policy and stops the matching process. Otherwise, the device continues to match packets against the next rule. If no rule is matched, the packets are allowed to pass through.

If an ACL contains multiple rules, packets match against the rules in the ascending order of rule IDs. If packets match a rule, the device considers that the ACL is matched and stops the matching process. Otherwise, the device continues to match packets against the next rule. If no rule is matched, the device considers that this ACL is not matched. To improve match efficiency, you are advised to configure an ACL rule with a high match probability first and set a small ID for the rule. This will reduce the number of times ACL rules are matched and save resources.

Prerequisites

An ACL rule has been created before this command is run.

- **acl (system view)**
- **acl name**

The device has been enabled to process STA IPv6 services of STAs using the **sta-ipv6-service enable** command.

Precautions

The **traffic-filter** command can reference a numbered ACL rule that is not configured. You can configure the referenced ACL rule after running this command.

You can only configure a maximum of eight ACL rules in the same direction. The sequence in which ACL rules takes effect follows the sequence in which the rules are configured. To change the current packet filtering rules, delete all the related configurations and reconfigure the ACL-based packet filtering.

Example

Create the traffic profile **p1** and configure packet filtering in the inbound direction based on the ACL that permits packets with the source IPv4 address 192.168.0.2/32.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-filter inbound ipv4 acl 3000
```

11.7.38 traffic-profile (WLAN view)

Function

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

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

By default, the system provides the traffic profile **default**.

Format

traffic-profile name *profile-name*

undo traffic-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a traffic profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all traffic profiles.	–

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

- The **traffic-profile** command applies to the following situations:
  - To apply priority mapping and traffic suppression functions to a VAP, create a traffic profile and bind the traffic profile to the VAP profile.
  - To change priority mapping and traffic suppression functions of a VAP, enter the traffic profile view of the VAP to modify the required parameters. When a traffic profile is not required, delete it.
- After a traffic profile is created, parameters in the profile use default values.

NOTE

- The profile name is mandatory when you create a profile.
- The traffic profile referenced by a VAP profile cannot be deleted. To delete the traffic profile, unbind it from the VAP profile first.

Example

Create traffic profile **p1** and display the traffic profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1]
```

11.7.39 traffic-profile (VAP profile view)

Function

The **traffic-profile** command binds a traffic profile to a VAP profile.

The **undo traffic-profile** command unbinds a traffic profile from a VAP profile.

By default, the traffic profile **default** is bound to a VAP profile.

Format

traffic-profile *profile-name*

undo traffic-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a traffic profile.	The traffic profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **traffic-profile** command to bind a traffic profile to a VAP profile. The traffic profile applies to all users using the VAP profile.

Prerequisites

The traffic profile has been created using the **traffic-profile (WLAN view)** command.

Example

Create VAP profile **p1** and bind traffic profile **u1** to the VAP profile.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name p1
[HUAWEI-wlan-vap-prof-p1] traffic-profile u1
```

11.7.40 traffic-remark (traffic profile view)

Function

The **traffic-remark** command configures ACL-based priority re-marking in a traffic profile.

The **undo traffic-remark** command cancels ACL-based priority re-marking in a traffic profile.

By default, ACL-based priority re-marking is not configured in a traffic profile.

Format

traffic-remark { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* } { **dot11e** *dot11e-value* | **dscp** *dscp-value* }

traffic-remark { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* } { **dot11e** *dot11e-value* | **dscp** *dscp-value* }

undo traffic-remark { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

undo traffic-remark { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based priority re-marking in the inbound direction.	-
outbound	Configures ACL-based priority re-marking in the outbound direction.	-
ipv4	Configures priority re-marking for IPv4 packets.	-
ipv6	Configures priority re-marking for IPv6 packets.	-
l2	Configures priority re-marking for Layer 2 packets.	-

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031 and from 6000 to 6031 for IPv4 ACLs, from 3000 to 3031 and 6000 to 6031 for an IPv6 ACLs, and from 4000 to 4031 for Layer 2 ACLs. • 3000 to 3031: advanced ACLs • 6000 to 6031: user ACLs • 4000 to 4031: Layer 2 ACLs
name *acl-name*	Re-marks packet priorities based on a specified named ACL. *acl-name* specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces and must begin with a letter. The value range of *acl-number* corresponding to *acl-name* is 3000 to 3031, and 6000 to 6031.
dot11e *dot11e-value*	Re-marks the 802.11e priority of packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
dscp *dscp-value*	Re-marks the DSCP priorities of packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The user wants to re-mark packet priorities based on ACLs to provide differentiated services. The **traffic-remark** command can be used to configure ACL-based priority re-marking.

Prerequisites

An ACL rule has been created before this command is run.

- **acl (system view)**
- **acl name**

The device has been enabled to process IPv6 services of STAs using the **sta-ipv6-service enable** command.

Precautions

The **traffic-remark** command can reference a numbered ACL rule that is not configured. You can configure the referenced ACL rule after running this command.

You can only configure a maximum of eight ACL-based packet re-marking rules in the same direction. The sequence in which ACL rules takes effect follows the rule configuration sequence. To change the current packet re-marking rules, delete all the related configurations and reconfigure the ACL-based packet re-marking.

When the **traffic-remark** command and the **traffic-filter (traffic profile view)** command are used simultaneously and the same ACL rule is associated:

- If the **deny** action is configured in the ACL rule, the **traffic-remark** command does not take effect.
- If the **permit** action is configured in the ACL rule, the command that is executed first takes effect.

Example

Create the traffic profile **p1** and configure ACL-based 802.11e priority re-marking for IPv4 packets in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-remark inbound ipv4 acl 3000 dot11e 7
```

11.7.41 ucc-profile (system view)

Function

The **ucc-profile** command creates a UCC profile and displays the UCC profile view, or displays the view of an existing UCC profile.

The **undo ucc-profile** command deletes a UCC profile.

By default, no UCC profile is created.

Format

ucc-profile name *profile-name*

undo ucc-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a UCC profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The string must start with a letter.
all	Indicates all UCC profiles.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. To ensure QoS guarantee for Lync packets and improve user experience, set the priority of Lync packets in the UCC profile.

Follow-up Procedure

Configure priorities of Lync voice, video, desktop sharing, and file transfer packets in the UCC profile and bind the UCC profile to a VAP profile.

Precautions

The UCC profile that has been bound to a VAP profile cannot be deleted. To delete the UCC profile, unbind the UCC profile from the VAP profile.

Example

Create a UCC profile named **test** and enter the UCC profile view.

```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test]
```

11.7.42 ucc-profile (VAP profile view)

Function

The **ucc-profile** command binds a UCC profile to a VAP profile.

The **undo ucc-profile** command unbinds a UCC profile from a VAP profile.

By default, no UCC profile is bound to a VAP profile.

Format

ucc-profile *profile-name*

undo ucc-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a UCC profile.	The UCC profile name must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

After a UCC profile is created, run the **ucc-profile** command to bind the UCC profile to a VAP profile so that the actions in the UCC profile take effect.

Example

Create a UCC profile named **test** and bind the UCC profile to the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] ucc-profile test
```

11.7.43 user-isolate (traffic profile view)

Function

The **user-isolate** command enables user isolation.

The **undo user-isolate** command disables user isolation.

By default, user isolation is disabled in a traffic profile.

Format

user-isolate l2

undo user-isolate

Parameters

Parameter	Description	Value
l2	Indicates user isolation at Layer 2 and communication at Layer 3.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a traffic profile, user isolation prevents packets of users on a VAP from being forwarded to each other. That is, users on the same VAP cannot communicate with each other after user isolation is enabled. This improves user communication security and enables the gateway to centrally forward user traffic, facilitating user management.

- In tunnel forwarding mode, user isolation in the traffic profile implements Layer 2 isolation for all users on a VAP.
- In direct forwarding mode, when enabling user isolation in the traffic profile, it is recommended that port isolation be deployed on the access switch port connected to the AP.

Example

Configure Layer 2 isolation and Layer 3 communication in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] user-isolate l2
Warning: Enabling user isolation may interrupt services. Are you sure you want to continue? [Y/N]:y
```

11.7.44 video remark

Function

The **video remark** command sets a priority for Lync video packets.

The **undo video remark** command deletes the priority of Lync video packets.

By default, the priority of Lync video packets is not set.

Format

video remark { **8021p** *8021p-value* | **dscp** { *dscp-value* | *dscp-name* } | **local-precedence** { *local-precedence-value* | *local-precedence-name* } }

undo video remark { **8021p** | **dscp** | **local-precedence** }

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
dscp { *dscp-value* | *dscp-name* }	Specifies the DSCP priority.	The value is a Diff-Serv code that is an integer ranging from 0 to 63, or a DSCP service type that can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values of service types are as follows: • af11: 10 • af12: 12 • af13: 14 • af21: 18 • af22: 20 • af23: 22 • af31: 26 • af32: 28 • af33: 30 • af41: 34 • af42: 36 • af43: 38 • cs1: 8 • cs2: 16 • cs3: 24 • cs4: 32 • cs5: 40 • cs6: 48 • cs7: 56 • default: 0 • ef: 46

Parameter	Description	Value
local-precedence { *local-precedence-value* | *local-precedence-name* }	Specifies the local priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. Or, the value is a service type that can be af1, af2, af3, af4, be, cs6, cs7, or ef. The values of service types are as follows: • af1: 1 • af2: 2 • af3: 3 • af4: 4 • be: 0 • cs6: 6 • cs7: 7 • ef: 5

Views

UCC profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. You can run the **video remark** command to change the priority of Lync video packets.

Precautions

The 802.1p priority and local priority cannot be set for the Lync video packets of one Lync session.

If you run the **video remark** command in the same UCC profile view multiple times to set the 802.1p priority, DSCP priority, or local priority of Lync video packets, only the latest configuration takes effect.

Example

Set the DSCP priority of Lync video packets to 1 in the UCC profile **test**.


```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] video remark dscp 1
```

11.7.45 voice remark

Function

The **voice remark** command sets a priority for Lync voice packets.

The **undo voice remark** command deletes the priority of Lync voice packets.

By default, the priority of Lync voice packets is not set.

Format

voice remark { **8021p** *8021p-value* | **dscp** { *dscp-value* | *dscp-name* } | **local-precedence** { *local-precedence-value* | *local-precedence-name* } }

undo voice remark { **8021p** | **dscp** | **local-precedence** }

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
dscp { *dscp-value* | *dscp-name* }	Specifies the DSCP priority.	The value is a Diff-Serv code that is an integer ranging from 0 to 63, or a DSCP service type that can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values of service types are as follows: • af11: 10 • af12: 12 • af13: 14 • af21: 18 • af22: 20 • af23: 22 • af31: 26 • af32: 28 • af33: 30 • af41: 34 • af42: 36 • af43: 38 • cs1: 8 • cs2: 16 • cs3: 24 • cs4: 32 • cs5: 40 • cs6: 48 • cs7: 56 • default: 0 • ef: 46

Parameter	Description	Value
local-precedence { *local-precedence-value* | *local-precedence-name* }	Specifies the local priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. Or, the value is a service type that can be af1, af2, af3, af4, be, cs6, cs7, or ef. The values of service types are as follows: • af1: 1 • af2: 2 • af3: 3 • af4: 4 • be: 0 • cs6: 6 • cs7: 7 • ef: 5

Views

UCC profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. You can run the **voice remark** command to change the priority of Lync voice packets.

Precautions

The 802.1p priority and local priority cannot be set for the Lync voice packets of one Lync session.

If you run the **voice remark** command in the same UCC profile view multiple times to set the 802.1p priority, DSCP priority, or local priority of Lync voice packets, only the latest configuration takes effect.

Example

Set the DSCP priority of Lync voice packets to 1 in the UCC profile **test**.


```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] voice remark dscp 1
```

11.7.46 wlan-slice high-reliability enable

Function

The **wlan-slice high-reliability enable** command enables WLAN high-reliability slicing.

The **undo wlan-slice high-reliability enable** command disables WLAN high-reliability slicing.

By default, the WLAN high-reliability slicing function is disabled.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability enable

undo wlan-slice high-reliability enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In industrial and healthcare scenarios, some latency-sensitive services exist. In this case, you can run the **wlan-slice high-reliability enable** command to enable the WLAN high-reliability slicing function. After this function is enabled, the AP allocates a period of time in the time domain to latency-sensitive services based on the air interface slicing configuration (expected RTT and slicing time proportion) to meet latency requirements of these services.

Precautions

- To ensure optimal air interface slicing, ensure that channel design, device selection, capacity planning, and position design comply with network planning and design requirements.

- In WLAN high-reliability slicing scenarios, if channels are manually planned, ensure that neighboring APs of any AP in the same frequency domain are invisible to each other, that is, no co-channel interference exists between the APs. For example, there are three APs in the same frequency domain: AP1 (neighbor of AP2), AP2 (neighbor of AP1 and AP3), and AP3 (neighbor of AP2). In this case, ensure that no co-channel interference exists between AP1 and AP3.
- When the WLAN high-reliability slicing function is enabled, terminal services may be interrupted.
- The WLAN high-reliability slicing function is mutually exclusive with the air scan function. After the WLAN high-reliability slicing function is enabled, AP radios do not support air scan, and scanning-dependent services, such as smart roaming, band steering, and load balancing, are unavailable.
- If the WLAN high-reliability slicing function is enabled on an AP, port isolation cannot be configured on the switch port connected to the AP.
- WLAN high-reliability slicing and interference visualization are not supported in Mesh scenarios.
- After WLAN high-reliability slicing is enabled in an RRM profile, the profile can be bound only to a 5 GHz radio profile. Each 5 GHz radio bound to this 5 GHz radio profile supports **a maximum of two VAPs**. As WLAN high-reliability slicing uses the VAP with the WLAN ID of 15, do not configure the WLAN ID of 15 for a service VAP.
- After WLAN high-reliability slicing is enabled, CoSR, MU-MIMO, and OFDMA do not take effect on the 2.4 GHz and 5 GHz radios.
- If the WLAN high-reliability slicing function is enabled but there are no low-latency services, high-priority slices cannot be properly utilized. As a result, spectral efficiency and performance deteriorate.
- To allow terminals connected to a Wi-Fi CPE to quickly go online, ensure that multicast traffic is not suppressed during deployment. After the deployment is complete, to ensure the delay of terminals connected to the Wi-Fi CPE, configure multicast traffic suppression on the AC's uplink interface (connected to an application server) and set the rate limit to 8 pps.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1 /////Assume that GE0/0/1 is the AC's uplink interface.
[HUAWEI-GigabitEthernet0/0/1] multicast-suppression packets 8
```

- CPEs need to stay in stationary state to ensure that air interface slicing reaches the optimal state.
- Do not deliver instructions to Wi-Fi CPEs in batches when air interface slicing is enabled.

Example

Enable WLAN high-reliability slicing.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] wlan-slice high-reliability enable
Warning: This operation will cause online STAs on the radio to go offline. Radios enabled with high-reliability air interface slicing can provide access only to CPEs with slicing capabilities. It is recommended that only one or two SSIDs be broadcast on a radio enabled with high-reliability air interface slicing. Because WLAN ID 15 of the radio is used for air interface slicing, specify other WLAN IDs as required.
Continue? [Y/N] y
```


11.7.47 wlan-slice high-reliability frer-enhance

Function

The **wlan-slice high-reliability frer-enhance** command enables the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios.

The **undo wlan-slice high-reliability frer-enhance** command disables the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios.

By default, the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios is disabled.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability frer-enhance

undo wlan-slice high-reliability frer-enhance

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Table 11-177 describes the recommended application scenarios of the enhanced dual fed and selective receiving function for WLAN high-reliability slicing.

Table 11-177 Application scenarios of the enhanced dual fed and selective receiving function for WLAN high-reliability slicing

Scenario	Enhanced Dual Fed and Selective Receiving Function for WLAN High-Reliability Slicing
There are a large number of STAs, and 2.4 GHz radios are heavily loaded. Only the performance indicator of 99.999% @ 20 ms is required.	Disabled
There are a small number of STAs, and high performance requirements are imposed. The performance indicator of higher than 99.999% @ 20 ms is required.	Enabled

NOTE

To achieve 99.999% @ 20 ms, the system must ensure that the RTT of only 1 in 100,000 packets exceeds 20 ms.

Prerequisites

The WLAN high-reliability slicing function has been enabled.

Example

Enable the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-view] wlan-slice high-reliability enable
Warning: This operation will cause online STAs on the radio to go offline. Radios enabled with high-reliability air interface slicing can provide access only to CPEs with slicing capabilities. It is recommended that only one or two SSIDs be broadcast on a radio enabled with high-reliability air interface slicing. Because WLAN ID 15 of the radio is used for air interface slicing, specify other WLAN IDs as required.
Continue? [Y/N] y
[HUAWEI-wlan-rrm-prof-p1] wlan-slice high-reliability frer-enhance
```

11.7.48 wlan-slice high-reliability rtt

Function

The **wlan-slice high-reliability rtt** command configures the expected round-trip time (RTT) of WLAN high-reliability slicing.

The **undo wlan-slice high-reliability rtt** command restores the default expected RTT of WLAN high-reliability slicing.

By default, the expected RTT of WLAN high-reliability slicing is 20 ms.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability rtt *rtt-value*

undo wlan-slice high-reliability rtt

Parameters

Parameter	Description	Value
rtt-value	Specifies the expected RTT value.	The value is an integer that ranges from 10 to 1000, in milliseconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this function is enabled, the AP allocates a period of time in the time domain to latency-sensitive services based on the air interface slicing configuration (expected RTT and slicing time proportion) to meet latency requirements of these services.

Example

Set the expected RTT of WLAN high-reliability slicing to 100 ms.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] wlan-slice high-reliability rtt 100
```


11.7.49 wlan-slice high-reliability time-ratio

Function

The **wlan-slice high-reliability time-ratio** command configures the time proportion for WLAN high-reliability slicing.

The **undo wlan-slice high-reliability time-ratio** command restores the default time proportion for WLAN high-reliability slicing.

The default time proportion for WLAN high-reliability slicing is 80%.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability time-ratio *time-ratio*

undo wlan-slice high-reliability time-ratio

Parameters

Parameter	Description	Value
time-ratio	Specifies the slicing time proportion.	The value is an integer that ranges from 0 to 80, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this function is enabled, the AP allocates a period of time in the time domain to latency-sensitive services based on the air interface slicing configuration (expected RTT and slicing time proportion) to meet latency requirements of these services.

Example

Set the time proportion for WLAN high-reliability slicing to 60%.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] wlan-slice high-reliability time-ratio 60
```

11.7.50 wlan-slice high-reliability acl

Function

The **wlan-slice high-reliability acl** command specifies an ACL for air interface slicing.

The **undo wlan-slice high-reliability acl** command deletes an ACL for air interface slicing.

By default, no ACL for air interface slicing is configured.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability { **ipv4** | **ipv6** | **l2** } **acl** *acl-number*

undo wlan-slice high-reliability { **ipv4** | **ipv6** | **l2** } **acl** *acl-number*

Parameters

Parameter	Description	Value
ipv4	Enables air interface slicing for IPv4 packets.	-
ipv6	Enables air interface slicing for IPv6 packets.	-
l2	Enables air interface slicing for Layer 2 packets.	-

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	For IPv4 and IPv6 ACLs, the value is an integer that ranges from 3000 to 3031 and 6000 to 6031 in the traffic profile. For Layer 2 ACLs, the value is an integer that ranges from 4000 to 4031. • 3000 to 3031: advanced ACLs • 6000 to 6031: user ACLs • 4000 to 4031: Layer 2 ACLs

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement QoS for multiple low-latency services in a more refined manner, you can enable the air interface slicing function for specific traffic. You can specify an ACL to filter traffic so that air interface slicing takes effect only for traffic that matches the ACL.

Air interface slicing identifies service traffic using access control lists (ACLs).

- Common terminal: Run the **wlan-slice high-reliability acl** command in the traffic profile to configure an ACL for air interface slicing. The device performs robust scheduling on the service traffic that matches the ACL.

Precautions

An ACL rule has been created before this command is run.

- **acl (system view)**
- **acl ipv6 (system view)**
- **acl name**
- **acl ipv6 name**

Example

Specify an ACL for air interface slicing in a traffic profile.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
```



```
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] wlan-slice high-reliability ipv4 acl 3000
```

11.7.51 wmm edca-ap

Function

The **wmm edca-ap** command sets EDCA parameters and ACK policies for an AP.

The **undo wmm edca-ap** command restores the default EDCA parameters and ACK policies for an AP.

Table 11-178 lists the default EDCA parameter settings and ACK policies for APs.

Table 11-178 Default EDCA parameter settings and ACK policies for APs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	3	2	1	47	normal
AC_VI	4	3	1	94	normal
AC_BE	6	4	3	0	normal
AC_BK	10	4	7	0	normal

Format

wmm edca-ap { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } } *

undo wmm edca-ap

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the AIFSN, which determines the channel idle time.	The value is an integer that ranges from 1 to 15.

Parameter	Description	Value
ecwmin *ecwmin-value*	Specifies the *ecwmin-value*. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be less than or equal to the *ecwmax-value* value.
ecwmax *ecwmax-value*	Specifies the *ecwmax-value*. *ecwmax-value* and *ecwmin-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than or equal to the *ecwmin-value* value.
txoplimit *txoplimit-value*	Specifies the TXOPLimit, which determines the maximum duration in which an AP or a STA can occupy a channel. A larger *txoplimit-value* value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. The unit is 32 microseconds. **NOTE** If the *txoplimit-value* value is 0, the STA can send only one data frame every time it occupies a channel.
ack-policy { **normal** | **noack** }	Specifies an ACK policy. • **normal**: During 802.11 packet exchange, the receiver must return an ACK packet each time it receives a packet from the sender. • **noack**: The receiver does not need to send an ACK message when it receives a packet from the sender. Configure this parameter only in the good air interface environment. Otherwise, severe packet loss occurs.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue. These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide different priorities for the packets. In this way, APs provide different capabilities to compete for channels, achieving differentiated services.

Precautions

- The EDCA parameters configured for the four AC queues take effect only after the WMM function is enabled. By default, the WMM function is enabled in a 2G or 5G radio profile.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.
- EDCA parameters must be configured properly. The scenarios for the reference EDCA parameter settings and ACK policies are as follows:
  a. Table 11-179 lists the reference EDCA parameter settings and ACK policies for APs in voice scenarios.

  Table 11-179 Reference EDCA parameter settings and ACK policies in voice scenarios

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	4	2	2	0	normal
AC_VI	5	3	5	0	normal
AC_BE	10	6	5	0	normal
AC_BK	10	8	12	0	normal

  b. Table 11-180 lists the reference EDCA parameter settings and ACK policies for APs in voice and video scenarios.

  Table 11-180 Reference EDCA parameter settings and ACK policies in voice and video scenarios

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	4	2	2	0	normal
AC_VI	5	3	5	0	normal
AC_BE	10	6	12	0	normal
AC_BK	10	8	12	0	normal

c. In high-density scenarios, it is recommended that you run the **dynamic-edca enable** command to enable dynamic EDCA parameter adjustment.

d. For other scenarios, the default settings are recommended.

Example

Set EDCA parameters and ACK policies for AC_VO packets in 5G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] wmm edca-ap ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit 0 ack-policy normal
```

11.7.52 wmm edca-client (SSID profile view)

Function

The **wmm edca-client** command configures EDCA parameters for STAs.

The **undo wmm edca-client** command restores the default EDCA parameter settings of STAs.

Table 11-181 lists the default EDCA parameter settings for STAs.

Table 11-181 Default EDCA parameter settings for STAs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit
AC_VO	3	2	2	47
AC_VI	4	3	2	94
AC_BE	10	4	3	0
AC_BK	10	4	7	0

Format

wmm edca-client { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw** **ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo wmm edca-client

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-

Parameter	Description	Value
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the arbitration inter frame spacing number (AIFSN), which determines the channel idle time.	The value is an integer that ranges from 12 to 15.
ecwmin *ecwmin-value*	Specifies the exponent form of the minimum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be less than or equal to the *ecwmax-value* value.
ecwmax *ecwmax-value*	Specifies the exponent form of the maximum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than or equal to the *ecwmin-value* value.
txoplimit *txoplimit-value*	Specifies the transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger TXOPLimit value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. The unit is 32 microseconds. **NOTE** If the TXOPLimit value is 0, the STA can send only one data frame every time it occupies a channel.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue.

These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide differentiated priorities to the packets and different capabilities to compete for channels. In this way, differentiated services are implemented.

Table 11-182 describes the EDCA parameters.

Table 11-182 EDCA parameter description

Parameter	Meaning
Arbitration Interframe Spacing Number (AIFSN)	The DIFS has a fixed value. WMM provides different DIFS values for different ACs. A large AIFSN value means that the STA must wait for a long time and has a low priority.
Exponent form of CWmin (ECWmin) and exponent form of CWmax (ECWmax)	ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. Together, they determine the average backoff time. Large ECWmin and ECWmax values mean a long average backoff time for the STA and a low STA priority.
Transmission Opportunity Limit (TXOPLimit)	After preempting a channel, the STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value means that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can only send one data frame every time it preempts a channel.

Precautions

- The EDCA parameters configured for the four AC queues take effect only after the WMM function is enabled using the **undo wmm disable** command.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.
- EDCA parameters must be configured properly. The scenarios for the reference EDCA parameter settings and ACK policies are as follows:
  a. Table 11-183 lists the reference EDCA parameter settings and ACK policies for APs in voice scenarios.

  Table 11-183 Reference EDCA parameter settings and ACK policies in voice scenarios

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	4	2	2	0	normal

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VI	5	3	5	0	normal
AC_BE	10	6	5	0	normal
AC_BK	10	8	12	0	normal

b. Table 11-184 lists the reference EDCA parameter settings and ACK policies for APs in voice and video scenarios.

Table 11-184 Reference EDCA parameter settings and ACK policies in voice and video scenarios

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	4	2	2	0	normal
AC_VI	5	3	5	0	normal
AC_BE	10	6	12	0	normal
AC_BK	10	8	12	0	normal

c. In high-density scenarios, it is recommended that you run the **dynamic-edca enable** command to enable dynamic EDCA parameter adjustment.

d. For other scenarios, the default settings are recommended.

Example

Set EDCA parameters for AC_VO packets of STAs in SSID profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name p1
[HUAWEI-wlan-ssid-prof-p1] wmm edca-client ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit 0
```

11.7.53 wmm mu-edca-client (SSID profile view)

Function

The **wmm mu-edca-client** command configures MU EDCA parameters for STAs.

The **undo wmm mu-edca-client** command restores the default MU EDCA parameter settings of STAs.

Table 11-185 lists the default MU EDCA parameter settings for STAs.

Table 11-185 Default MU EDCA parameter settings for STAs

Packet Type	ECWmax	ECWmin	AIFSN	MUEDCATimer
AC_VO	3	2	2	1
AC_VI	4	3	2	1
AC_BE	10	4	3	1
AC_BK	10	4	7	1

Format

wmm mu-edca-client { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw** **ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **muedcatimer** *muedcatimer-value* } *

undo wmm mu-edca-client

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the arbitration inter frame spacing number (AIFSN), which determines the channel idle time.	The value is an integer that ranges from 2 to 15.
ecwmin *ecwmin-value*	Specifies the exponent form of the minimum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be less than or equal to *ecwmax-value*.
ecwmax *ecwmax-value*	Specifies the exponent form of the maximum contention window. *ecwmax-value* and *ecwmin-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than or equal to *ecwmin-value*.

Parameter	Description	Value
muedcatimer *muedcatimer-value*	Specifies the MU EDCA timer, indicating the validity duration of MU EDCA parameters. When the timer is 0, the conventional EDCA parameters take effect.	The value is an integer that ranges from 1 to 255, in the unit of 8 TUs (1 TU = 1024 us).

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

STAs in compliance with 802.11ax or later standards (Wi-Fi 6/7 STAs) support two transmission modes: EDCA-based contention transmission and Trigger frame-based uplink transmission. In this way, Wi-Fi 6/7 STAs have more channel access opportunities than legacy STAs. To ensure channel access fairness, the MU EDCA mechanism is introduced. After being triggered by the AP to send data, Wi-Fi 6/7 STAs switch to the MU EDCA parameter set. The MU EDCA parameter set has a longer contention waiting time and a larger backoff window, and therefore has a lower priority compared with the conventional EDCA parameter set.

If Wi-Fi 6/7 STAs do not schedule Trigger frames for a long time, the STAs exit the MU EDCA mechanism and switch back to conventional EDCA parameters.

Precautions

Improper settings for MU EDCA parameters may cause poor uplink user experience.

In most scenarios, the default configurations are recommended. In MU scenarios, the recommended configurations are described in the following table.

Table 11-186 Recommended MU EDCA parameter settings for STAs in MU scenarios

Packet Type	ECWmax	ECWmin	AIFSN	MUEDCATimer
AC_VO	3	2	3	1
AC_VI	4	3	3	1
AC_BE	10	4	4	1

Packet Type	ECWmax	ECWmin	AIFSN	MUEDCATimer
AC_BK	10	4	8	1

Example

Set MU EDCA parameters for AC_VO packets of STAs in the SSID profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name p1
[HUAWEI-wlan-ssid-prof-p1] wmm mu-edca-client ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 muedcatimer 1
```

11.7.54 wmm disable (radio profile view)

Function

The **wmm disable** command disables the Wi-Fi Multimedia (WMM) function in a 2G or 5G radio profile.

The **undo wmm disable** command enables the WMM function in a 2G or 5G radio profile.

By default, the WMM function is enabled in a 2G or 5G radio profile.

Format

wmm disable

undo wmm disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

802.11be, 802.11ax, 802.11ac and 802.11n STAs must support WMM. If the WMM function is disabled on a radio, 802.11be, 802.11ax, 802.11ac and 802.11n cannot work and STAs can access the network only in 802.11a/b/g mode.

If the WMM function is disabled, the access of non-HT STAs fails to be denied.

After the WMM function is enabled in a 2G or 5G radio profile, the AP radio to which the 2G or 5G radio profile is applied can use the WMM parameters.

Example

Enable the WMM function in 5G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] undo wmm disable
```

11.7.55 wmm mandatory enable

Function

The **wmm mandatory enable** disables STAs that do not support WMM from connecting to a WMM-enabled AP.

The **undo wmm mandatory enable** allows STAs that do not support WMM to connect to a WMM-enabled AP.

By default, STAs that do not support WMM are allowed to connect to a WMM-enabled AP.

Format

wmm mandatory enable

undo wmm mandatory enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

On a WLAN, wireless channels are open and all STAs have the same chance to occupy a channel. You can configure WMM to distinguish high-priority packets and enable the high-priority packets to preempt channels. You can also disable STAs that do not support WMM from connecting to a WMM-enabled AP, which prevents those STAs from preempting channels of WMM-capable STAs.

Example

Disable STAs that do not support WMM to connect to a WMM-enabled AP.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] wmm mandatory enable
```

11.8 DFI Configuration Commands

11.8.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

NOTE

The DFI function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD)
- AirEngine X762 series APs running V200R021C10 or later
- AirEngine X771 series APs
- AirEngine 9700D-S (including matching ORUs)

11.8.2 dynamic flow inspection

Function

The **dynamic flow inspection** command enables or disables DFI on a VAP.

The **undo dynamic flow inspection** command restores the default DFI state on a VAP.

By default, DFI is disabled on AirEngine 5762S series models and enabled on other AP models.

Format

dynamic flow inspection { **enable** | **disable** }

undo dynamic flow inspection

Parameters

Parameter	Description	Value
enable	Enables the DFI function.	-
disable	Disables the DFI function.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the DFI function is enabled on a VAP, the device identifies the traffic on this VAP and preferentially guarantees the downlink traffic of gaming and VoIP services on the air interface based on the identification result.

Precautions

Disabling the DFI function may cause the game turbo function to become invalid.

Example

Enable the DFI function on a VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name default
[HUAWEI-wlan-vap-prof-default] dynamic flow inspection enable
```

11.9 Application Identification Configuration Commands

11.9.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.9.2 application-group car (SAC profile view)

Function

The **application-group car** command enables rate limiting on a specified application group or a specified application in the group.

The **undo application-group car** command disables rate limiting on a specified application group or a specified application in the group.

By default, rate limiting is not configured for packets of any application in an application group.

Format

application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **car** *cir-value*

undo application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **car**

Parameters

Parameter	Description	Value
application-group *group-name*	Specifies the name of an application group.	The specified application group name must exist in the SAC signature file.
app-protocol *app-protocol-name*	Specifies the name of an application.	The specified application must exist.
all	Specifies all applications in the group.	-
car *cir-value*	Specifies the committed information rate (CIR).	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to enable rate limiting on all applications in a group or the specified application in the group.

Precautions

If **application-group remark (SAC profile view)** or **application-group car (SAC profile view)** and **application-group deny (SAC profile view)** are both configured for an application, the rate limit and priority modification policy do not take effect for the application protocol packets, and the packets are discarded.

Prerequisites

Example

Set the CIR value to 100 kbit/s of the application in the application group in the SAC profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] application-group  app-protocol  car 100
```

11.9.3 application-group deny (SAC profile view)

Function

The **application-group deny** command enables the device to discard packets of all applications in an application group or a specific application in the group.

The **undo application-group deny** command disables the device from discarding packets of all applications in an application group or a specific application in the group.

By default, the device does not discard packets of any application in an application group.

Format

application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **deny**

undo application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **deny**

Parameters

Parameter	Description	Value
application-group *group-name*	Specifies the name of an application group.	The specified application group name must exist in the SAC signature file.
app-protocol *app-protocol-name*	Specifies the name of an application.	The specified application must exist.
all	Specifies all applications in the group.	-

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A WLAN transmits traffic of varied applications. The network administrator needs to know traffic usage of the applications to plan network capacity and locate problems on the network. In this situation, you can take application traffic control measures. If packets of a specified application need to be discarded, run the **application-group deny** command. You can also use the command to discard packets of a specified protocol type or a protocol type in a specified application group.

Precautions

If **application-group remark (SAC profile view)** or **application-group car (SAC profile view)** and **application-group deny (SAC profile view)** are both configured for an application, the rate limit and priority modification policy do not take effect for the application protocol packets, and the packets are discarded.

Prerequisites

Example

Configure the device to discard packets of the application in the SAC profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] application-group  app-protocol  deny
```

11.9.4 application-group remark (SAC profile view)

Function

The **application-group remark** command re-marks packet priorities based on a specific application group or a specific application in the group.

The **undo application-group remark** command cancels packet priority remarking based on a specific application group or a specific application in the group.

By default, an action of re-marking packet priorities based on a specific application group or a specific application in the group is not configured in an SAC profile view.

Format

application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **remark** { **dscp** *dscp-value* | **dot1p** *dot1p-value* }

undo application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **remark** { **dscp** | **dot1p** }

Parameters

Parameter	Description	Value
application-group *group-name*	Specifies the name of an application group.	The specified application group name must exist in the SAC signature file.
app-protocol *app-protocol-name*	Specifies the name of an application.	The specified application must exist.
all	Re-marks priorities of packets of all applications in the group.	-
dscp *dscp-value*	Specifies the DSCP priority.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
dot1p *dot1p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **application-group remark** command to re-mark packet priorities based on a specific application group or a specific application in the group. In this way, different user packets are granted the same priority, facilitating flexible user management.

Precautions

If **application-group remark (SAC profile view)** or **application-group car (SAC profile view)** and **application-group deny (SAC profile view)** are both configured for an application, the rate limit and priority modification policy do not take effect for the application protocol packets, and the packets are discarded.

Before running this command, ensure that the mode of mapping 802.3 packets (sent by upper-layer devices to APs) to 802.11 packets is the same as the packet priority re-marking type you want to configure. Specifically:

- Run the **priority-map downstream trust dot1p** command if you want to specify the parameter **dot1p** *dot1p-value*.
- Run the **priority-map downstream trust dscp** command (default) if you want to specify the parameter **dscp** *dscp-value*.

Prerequisites

Example

Re-mark DSCP priorities of packets of the application in the SAC profile **p1** as 30.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] application-group  app-protocol  remark dscp 30
```

11.9.5 category sub-category (AP user-defined application view)

Function

The **category sub-category** command configures the category and subcategory of an AP user-defined application.

The **undo category** command restores the default category and subcategory of an AP user-defined application.

The default category and subcategory of an AP user-defined application are **General** and **Other**, respectively.

Format

category *category* **sub-category** *sub-category*

undo category

Parameters

Parameter	Description	Value
category	Specifies the category of an application.	The specified category must be supported by the device.
sub-category	Specifies the subcategory of an application.	The specified subcategory must be supported by the device.

Views

AP user-defined application view

Default Level

2: Configuration level

Usage Guidelines

One category contains multiple subcategories, but one subcategory belongs to only one category.

During the configuration, you can enter a question mark (?) to display the supported categories and subcategories.

Example

Set the category and subcategory of the AP user-defined application **UD_abc** to **Business_Systems** and **Database**, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] category Business_Systems sub-category Database
```

11.9.6 defence engine enable ap-group

Function

The **defence engine enable ap-group** command enables the security engine for AP groups.

The **undo defence engine enable ap-group** command disables the security engine for AP groups.

By default, the security engine is disabled for an AP group.

Format

defence engine enable ap-group { **all** | **name** *ap-group-name* }

undo defence engine enable ap-group { **all** | **name** *ap-group-name* }

Parameters

Parameter	Description	Value
all	Enables or disables the security engine for all AP groups.	-
name *ap-group-name*	Enables or disables the security engine for the AP group with a specified name.	The AP group must exist.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a WLAN, if you need to monitor applications in real time, collect application traffic statistics, or perform QoS scheduling, run the **defence engine enable ap-group** command to enable the security engine for AP groups.

Precautions

After the **defence engine enable ap-group all** command is run to enable the security engine for all AP groups, you cannot disable the security engine for only a specified AP group. Instead, you can only run the **undo defence engine enable ap-group all** command to disable the security engine for all AP groups.

Example

Enable the security engine for the AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable ap-group name default
```

11.9.7 description (AP user-defined application rule view)

Function

The **description** command configures the description for an AP user-defined application rule.

The **undo description** command deletes the description of an AP user-defined application rule.

By default, no description is configured for a new AP user-defined application rule.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an AP user-defined application rule.	The value is a string of 1 to 128 case-sensitive characters, spaces supported.

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the description for an AP user-defined application rule.

Example

Configure the description **test** for the AP user-defined application rule **rule1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] description test
```

11.9.8 description (AP user-defined application view)

Function

The **description** command configures the description for an AP user-defined application.

The **undo description** command deletes the description of an AP user-defined application.

By default, no description is configured for a new AP user-defined application.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an AP user-defined application.	The value is a string of 1 to 128 case-sensitive characters, spaces supported.

Views

AP user-defined application view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the description for an AP user-defined application.

Example

Configure the description **test** for the AP user-defined application **UD_abc**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] description test
```

11.9.9 destination-port (AP user-defined application rule view)

Function

The **destination-port** command configures a port number for an AP user-defined application rule.

The **undo destination-port** command deletes the port number of an AP user-defined application rule.

By default, no port number is configured for a new AP user-defined application rule.

Format

destination-port *port*

undo destination-port

Parameters

Parameter	Description	Value
port	Specifies the port number for an AP user-defined application rule.	The value is an integer that ranges from 1 to 65535.

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

After a port number is configured using this command, the service awareness (SA) engine will match network packets based on the configured port number as well as the transport-layer protocol and IP address (that is, 3-tuple information). If destination 3-tuple information about the traffic to be identified is determined, you can configure user-defined 3-tuple information to accelerate identification. For example, you can configure a 3-tuple user-defined rule based on the IP address, port number, and transport-layer protocol of a server, so that the rule can identify all the traffic accessing this server. A triplet rule must contain at least either one IP address or one port number. Note that only the destination port number can be specified in this command configuration.

Example

Configure the port number **80** for the AP user-defined application rule **rule1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] destination-port 80
```

11.9.10 display ap application

Function

The **display ap application** command displays information about applications on APs.

Format

display ap application

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view information about all applications on APs.

Prerequisites

The security engine has been enabled for the specified AP group using the **defence engine enable ap-group** command.

Example

Display information about applications on APs.

```
<HUAWEI> display ap application
-------------------------------------------------------------------------------------------------------------
 AppID   Name                        Sub-category
-------------------------------------------------------------------------------------------------------------
 1       bt                        fileshare_p2p
 3       thunder                     fileshare_p2p
 5       ftp                       infrastructure
 6       ftps                      infrastructure
 9       qqlive                     peercasting
 15      kugoo                        peercasting
 41      qq_voip                      voip
 45      qq_im                        instant_message
.....
-------------------------------------------------------------------------------------------------------------
 Total: 188
```

Table 11-187 Description of the **display ap application** command output

Item	Description
AppID	Application ID.
Name	Application name.
Sub-category	Subcategory to which an application belongs.

11.9.11 display ap application-group

Function

The **display ap application-group** command displays information about application groups on APs.

Format

display ap application-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays information about a specified application group. If this parameter is not specified, information about all application groups on APs is displayed.	The specified application group name must be supported by the application identification signature database file.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view information about all application groups or a specified application list on APs.

Prerequisites

The security engine has been enabled for the specified AP group using the **defence engine enable ap-group** command.

Example

Display information about all application groups on APs.

```
<HUAWEI> display ap application-group
----------------------------------------
  Index       GroupName
----------------------------------------
  1           auth_service
  2           finance
  3           data_backup
  4           database
  5           email
  6           enterprise_application
  7           internet_conferencing
  8           remote_access
  9           game
  10          instant_messaging
----------------------------------------
 Total: 10
```

Display information about the application group **email**.

```
<HUAWEI> display ap application-group email
----------------------------------
```



```
  Index    Application name
-----------------------------------
  9951     WebMail_AliyunMail
  10062    Webmail_DingTalkMail
  10528    Foxmail
-----------------------------------
  Total: 3
```

Table 11-188 Description of the **display ap application-group** command output

Item	Description
Index	Sequence number of an application protocol in the application group.
GroupName	Name of the application group.
Application name	Name of an application protocol in the application group.

11.9.12 display apsa-sdb

Function

The **display apsa-sdb** command displays information about the AP application identification signature database.

Format

display apsa-sdb { **version** | **update information** }

Parameters

Parameter	Description	Value
version	Displays the version of the application identification signature database.	-
update information	Displays update information about the application identification signature database.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Before and after updating the application identification signature database, you can run the **display apsa-sdb** { **version** | **update information** } command to view the version and update information of the signature database and check whether the update is successful.

Prerequisites

The security engine has been enabled for the specified AP group using the **defence engine enable ap-group** command.

Example

Display the version of the AP application identification signature database.

```
<HUAWEI> display apsa-sdb version
-------------------------------------------------------------
Current Version:
  Signature Database Version:2021032403
  Signature Database Size(byte):132897
  Update Time:2021-06-22 06:16:42
  Issue Time of the Update File:2021-03-24 10:11:23
-------------------------------------------------------------
```

Table 11-189 Description of the **display apsa-sdb version** command output

Item	Description
Current Version	The current signature database version is displayed in the following information.
Signature Database Version	Signature database version.
Signature Database Size(byte)	Signature database size.
Update Time	Update time of the signature database, that is, the installation time of the update package.
Issue Time of the Update File	Issue time of the update file, showing whether the update package is the latest.

Display update information about the AP application identification signature database.

```
<HUAWEI> display apsa-sdb update information
Current Update Status:  Idle.
-----------------------------------------------------
  Latest update finish time : 2021-06-22006:16:42
  Latest update result : success
 -----------------------------------------------------
```


Table 11-190 Description of the **display apsa-sdb update information** command output

Item	Description
Current Update Status	Current status of the update server. • Idle: No signature database is being updated. • Version Loading: The version is being loaded. • Live Updating: The online update is in progress. • Local Updating: The local update is in progress. • Version Rollbacking: The version is being rolled back. • Stop Updating: The update is being canceled. • Version Applying: The version is being downloaded and installed. • Version Restoring: The default version is being restored. • Version Uninstalling: The version is being uninstalled. • Update check: The update is being checked. • Engine start loading: The security engine is being loaded.
Latest update finish time	Last update finish time of the signature database.
Latest update result	Last update result of the signature database.

11.9.13 display defence engine configuration

Function

The **display defence engine configuration** command displays whether the security engine is enabled for APs.

Format

display defence engine configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **defence engine enable ap-group** command to enable the security engine for AP groups, you can run this command to check whether the security engine is enabled for APs.

Example

Display whether the security engine is enabled for APs.

```
<HUAWEI> display defence engine configuration
AP group engine state : all
-------------------------------------------------------------
Group name                  State
-------------------------------------------------------------
default                     Disable
-------------------------------------------------------------
Total items displayed: 1
```

Table 11-191 Description of the **display defence engine configuration** command output

Item	Description
AP group engine state	Security engine state of AP groups. This field is displayed as **all** only when the security engine is enabled for all AP groups. Otherwise, no information is displayed for this field.
Group name	AP group name.
State	Whether the security engine is enabled for an AP group. • Enable: The security engine is enabled. • Disabled: The security engine is disabled.

11.9.14 display references sac-profile

Function

The **display references sac-profile** command displays the reference information of an SAC profile.

Format

display references sac-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays the reference information of a specified SAC profile.	The SAC profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the profiles by which a specified SAC profile is referenced.

Example

Display the reference information of the SAC profile **p1**.

```
<HUAWEI> display references sac-profile name p1
-------------------------------------------------------
Reference type     Reference name
-------------------------------------------------------
VAP profile        wlan-vap
-------------------------------------------------------
Total: 1
```

Table 11-192 Description of the **display references sac-profile** command output

Item	Description
Reference type	Type of the profile that references an SAC profile.
Reference name	Name of the profile that references an SAC profile.

11.9.15 display wlan sac-profile

Function

The **display wlan sac-profile** command displays configuration and reference information about SAC profiles.

Format

display wlan sac-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all SAC profiles.	-
name *profile-name*	Displays information about the SAC profile with a specified name.	The SAC profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display sac-profile** command to view the configuration and reference information about SAC profiles.

Example

Display information about all SAC profiles.

```
<HUAWEI> display wlan sac-profile all
------------------------------------------------------------
Profile name                Reference
------------------------------------------------------------
u1                          0
------------------------------------------------------------
Total: 1
```

Table 11-193 Description of the **display wlan sac-profile all** command output

Item	Description
Profile name	Name of an SAC profile.
Reference	Number of times an SAC profile is referenced.

Display information about the SAC profile **u1**.

```
<HUAWEI> display wlan sac-profile name u1
------------------------------------------------------------------------------
SAC Profile name                : u1
```



```
User statistic                : disable
VAP statistic                 : disable
SAC Policy
------------------------------------------------------------------------------
```

Table 11-194 Description of the **display wlan sac-profile name** command output

Item	Description
SAC Profile name	Name of an SAC profile. To configure this parameter, run the **sac-profile** command.
User statistic	User protocol statistics collection function. To configure this parameter, run the **user-protocol-statistic enable** command.
VAP statistic	Protocol statistics collection function on VAPs. To configure this parameter, run the **vap-protocol-statistic enable** command.
SAC Policy	SAC policy based on the protocol application or protocol application groups. To configure this parameter, run the **application-group car (SAC profile view)**, **application-group deny (SAC profile view)**, or **application-group remark (SAC profile view)** command.

11.9.16 display sac application user-defined

Function

The **display sac application user-defined** command displays user-defined applications deployed on an AP.

Format

display sac application user-defined { **id** *application-id* | **name** *name* | **all** }

Parameters

Parameter	Description	Value
id *application-id*	Specifies the ID of an AP user-defined application.	The value is an integer that ranges from 65000 to 65031.
name *name*	Specifies the name of an AP user-defined application.	The value is a string of case-sensitive characters, and must start with **UD_**. If the name does not contain spaces, the value is a string of 4 to 32 characters. If the name contains spaces, the value is a string of 6 to 34 characters and must be enclosed with double quotation marks (""), for example, **"UD_user for test"**. The name cannot contain question marks (?), commas (,), or hyphens (-). If the name does not contain any space, it also cannot contain double quotation marks (").
all	Displays all AP user-defined applications.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

You can run this command to view the configuration of user-defined applications deployed on an AP.

Example

Display all AP user-defined applications.

```
<HUAWEI> display sac application user-defined all
------------------------------------------------------------------------------
AppID Name                      Category                Sub-category
------------------------------------------------------------------------------
65000 UD_abc                    general                 other
------------------------------------------------------------------------------
Total: 1
```


Table 11-195 Description of the **display sac application user-defined all** command output

Item	Description
AppID	ID of an AP user-defined application.
Name	Name of an AP user-defined application.
Category	Category of an AP user-defined application.
Sub-category	Subcategory of an AP user-defined application.

Display the configuration of the AP user-defined application **UD_abc**.

```
<HUAWEI> display sac application user-defined name UD_abc
------------------------------------------------------------------------------
User-defined application configuration:
Name            : UD_abc
ID              : 65000
Category        : general
Sub-category    : other

Rule configuration:
Rule number     : 1
Rule name       : rule1
Rule id         : 0
Rule state      : success
   IP address              : 0.0.0.0/0
   Destination port        : 0
   Protocol                : tcp
   Signature type          : packet
   Signature direction     : both
   Signature plain-string  : abcdf
------------------------------------------------------------------------------
```

Table 11-196 Description of the **display sac application user-defined** command output

Item	Description
User-defined application configuration	
Name	Name of the AP user-defined application.
ID	ID of the AP user-defined application.
Category	Category of the AP user-defined application.
Sub-category	Subcategory of the AP user-defined application.
Description	Description of the AP user-defined application.

Item	Description
Rule configuration	
Rule number	Number of AP user-defined application rules.
Rule name	Name of an AP user-defined application rule.
Rule id	ID of an AP user-defined application rule.
Rule state	Rule delivery result. ● success: The rule is delivered successfully. ● failed: The rule delivery fails. ● committing: The rule is being delivered.
IP address	IPv4 address and subnet mask of an AP user-defined application rule.
Destination port	Port number of an AP user-defined application rule.
Protocol	Transport-layer protocol type of an AP user-defined application rule.
Signature type	Detection scope: ● packet
Signature direction	Detection direction: ● both: both request and response directions ● request: request direction ● response: response direction
Signature plain-string	Configured keyword.

11.9.17 ip-address (AP user-defined application rule view)

Function

The **ip-address** command configures an IPv4 address for an AP user-defined application rule.

The **undo ip-address** command deletes the IPv4 address of an AP user-defined application rule.

By default, no IPv4 address is configured for a new AP user-defined application rule.

Format

ip-address *ip-address* [*mask* | *mask-length*]

undo ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
mask	Specifies the subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer in the range from 1 to 32.

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

You can configure a single IPv4 address for a user-defined application rule, or configure a network segment by specifying the subnet mask or mask length.

After an IPv4 address is configured using this command, the service awareness (SA) engine will match network packets based on the configured IPv4 address as well as the transport-layer protocol and port number (that is, 3-tuple information). If destination 3-tuple information about the traffic to be identified is determined, you can configure user-defined 3-tuple information to accelerate identification. For example, you can configure a 3-tuple user-defined rule based on the IP address, port number, and transport-layer protocol of a server, so that the rule can identify all the traffic accessing this server. A triplet rule must contain at least either one IP address or one port number. Note that only the destination IPv4 address can be specified in this command configuration.

Example

Configure the IPv4 address **10.1.1.1** for the user-defined application rule **rule1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] ip-address 10.1.1.1
```


11.9.18 priority-remark-default

Function

The **priority-remark-default** command enables the device to restore the default priorities of SAC applications.

The **undo priority-remark-default** command disables the device from restoring the default priorities of SAC applications.

By default, the device restores the default priorities of SAC applications.

Format

priority-remark-default

undo priority-remark-default

Parameters

None

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SAC function allows you to modify the priorities of application packets as required. However, defining the priorities of applications one by one is not user-friendly.

After this command is executed, the default priorities of all applications identified by SAC are restored based on the identification result. This ensures that applications that require high real-timeness and reliability have higher priorities when SAC is enabled.

To check the default priorities of different applications, run the **display sac default-priority** command.

Example

Enable the device to restore the default priorities of SAC applications.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI--wlan-sac-prof-p1] priority-remark-default
```


11.9.19 protocol (AP user-defined application rule view)

Function

The **protocol** command configures the transport-layer protocol for an AP user-defined application rule.

The **undo protocol** command restores the default transport-layer protocol of an AP user-defined application rule.

By default, the transport-layer protocol of an AP user-defined application rule is any, that is, the rule takes effect for both TCP and UDP packets.

Format

protocol { **tcp** | **udp** }

undo protocol

Parameters

Parameter	Description	Value
tcp	Specifies the TCP protocol.	-
udp	Specifies the UDP protocol.	-

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to configure the transport-layer protocol for an AP user-defined application rule. To make the rule take effect, however, you also need to specify other configuration items.

Example

Configure TCP as the transport-layer protocol of an AP user-defined application rule.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] protocol tcp
```


11.9.20 rule name (AP user-defined application view)

Function

The **rule name** command configures a rule for an AP user-defined application and displays the rule view.

The **undo rule** command deletes rules of an AP user-defined application.

By default, no rule is configured for a new AP user-defined application.

Format

rule name *name*

undo rule { **name** *name* | **all** }

Parameters

Parameter	Description	Value
name *name*	Specifies the rule name.	The name is a string of case-sensitive characters. If the name does not contain spaces, the value is a string of 1 to 32 characters. If the name contains spaces, the value is a string of 3 to 34 characters and must be enclosed with double quotation marks (""), for example, **"user for test"**. The name cannot contain question marks (?), commas (,), or hyphens (-). If the name does not contain any space, it also cannot contain double quotation marks ("). The name cannot be **any** or **all**.
all	Deletes all AP user-defined application rules.	-

Views

AP user-defined application view

Default Level

2: Configuration level

Usage Guidelines

If the specified rule name of an AP user-defined application does not exist, a new rule is created for the AP user-defined application and the rule view is displayed. If the specified rule name of the AP user-defined application already exists, the rule view is directly displayed.

A rule can be created based on 3-tuple information, keywords, or both 3-tuple information and keywords. The 3-tuple information refers to the server IP address, protocol type, and destination port number. The keywords are signatures of data packets or data flows corresponding to an application and uniquely identify the application.

- You can run the **ip-address (AP user-defined application rule view)**, **destination-port (AP user-defined application rule view)**, and **protocol (AP user-defined application rule view)** commands to specify 3-tuple information for an application.
- You can run the **signature (AP user-defined application rule view)** command to specify keywords for an application.

Multiple rules can be configured for one AP user-defined application. These rules are logically ORed. Data flows or packets belong to the application once they match one of the rules.

If the number of user-defined application rules on an AP reaches the maximum but the number of user-defined applications does not reach the maximum, you can continue to configure user-defined applications but cannot configure new rules for these applications.

Example

Create the rule **rule1** for the AP user-defined application **UD_abc** and display the rule view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1]
```

11.9.21 sac-profile

Function

The **sac-profile** command creates an SAC profile and displays the SAC profile view, or displays the view of an existing SAC profile.

The **undo sac-profile** command deletes an SAC profile. To delete a bound SAC profile, unbind the profile first.

By default, no SAC profile is available in the system.

Format

sac-profile name *profile-name*

undo sac-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an SAC profile.	The value is a string of 1 to 35 case-insensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all SAC profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **sac-profile** command to create an SAC profile. In the profile, you can perform the following configurations: discarding traffic of specified applications, setting priorities for packets of specified applications, and limiting packet rate of specified applications.

Example

Create the SAC profile **p1** and enter the SAC profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1]
```

11.9.22 signature (AP user-defined application rule view)

Function

The **signature** command configures the signature for an AP user-defined application.

The **undo signature** command deletes the signature of an AP user-defined application.

By default, no signature is configured for an AP user-defined application.

Format

signature context packet direction { **request** | **response** | **both** } **plain-string** *plain-string*

undo signature

Parameters

Parameter	Description	Value
context	Specifies the context with which the signature to be configured matches.	-
packet	Indicates the packet-based matching mode.	-
request	Indicates the request detection direction.	-
response	Indicates the response detection direction.	-
both	Indicates that the detection direction is both request and response directions.	-
plain-string *plain-string*	Indicates a plain-text string.	The value is a string of 3 to 128 case-sensitive characters. If the string contains spaces and question marks (?), the value is a string of 5 to 130 characters and must be enclosed with double quotation marks (""), for example, **"GET w?"**. If the string contains a double quotation mark ("), the double quotation mark needs to be escaped into **\x22**. For example, if the string is **abc"d**, you need to enter **abc\x22d**.

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

Only one signature can be configured for an AP user-defined application rule.

If you run this command multiple times, only the latest configuration takes effect.

Example

Configure the signature **abcde** for the AP user-defined application rule **rule1**, configure the packet-based matching mode, and set the detection direction to the request direction.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] protocol tcp
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] signature context packet direction request plain-string abcde
```

11.9.23 sac-profile (VAP profile view)

Function

The **sac-profile** command binds an SAC profile to a VAP profile.

The **undo sac-profile** command unbinds an SAC profile to a VAP profile.

By default, no SAC profile is bound to a VAP profile.

Format

sac-profile *profile-name*

undo sac-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an SAC profile.	The SAC profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to bind an SAC profile to a VAP profile. The SAC profile then applies to all users using this VAP profile.

Example

Bind the SAC profile **p1** to the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] quit
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] sac-profile p1
```

11.9.24 upgrade local apsa-sdb

Function

The **upgrade local apsa-sdb** command manually updates the local application signature database for APs.

Format

upgrade local apsa-sdb file *filename*

Parameters

Parameter	Description	Value
file *filename*	Specifies the update file, in .zip format. You need to upload the file to the flash directory of the storage device through FTP or SFTP in advance.	The value is a string of 1 to 64 characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To update the signature database, download the update file from Huawei security center isecurity.huawei.com to the PC, upload the file to the flash directory of the storage device through FTP or SFTP, and then run this command to update the signature database.

Prerequisites

The security engine has been enabled for the specified AP group using the **defence engine enable ap-group** command.

Precautions

The update file must be placed in the flash directory, because this command does not support the file path setting.

This command cannot be used to load the signature database for APs running V200R019C00 or earlier.

Example

Manually update the local application signature database for APs using the signature file **APSA_H30071006_2021053106.zip**.

```
<HUAWEI> system-view
[HUAWEI] upgrade local apsa-sdb file APSA_H30071006_2021053106.zip
Warning: This operation will upgrade the AP signature database file. Continue? [Y/N]:y
It will take several seconds to update the AP signature database file, please wait.....
Info: The AP signature database file is successfully upgraded.
```

11.9.25 user-defined-application (WLAN view)

Function

The **user-defined-application** command creates an AP user-defined application and displays the AP user-defined application view.

The **undo user-defined-application** command deletes AP user-defined applications.

By default, no AP user-defined application is configured.

Format

user-defined-application id *application-id* [**name** *name*]

undo user-defined-application { **id** *application-id* | **name** *name* | **all** }

Parameters

Parameter	Description	Value
id *application-id*	Specifies the ID of an AP user-defined application.	The value is an integer that ranges from 65000 to 65031.

Parameter	Description	Value
name *name*	Specifies the name of an AP user-defined application.	The value is a string of case-sensitive characters, and must start with **UD_**. If the name does not contain spaces, the value is a string of 4 to 32 characters. If the name contains spaces, the value is a string of 6 to 34 characters and must be enclosed with double quotation marks (""), for example, **"UD_user for test"**. The name cannot contain question marks (?), commas (,), or hyphens (-). If the name does not contain any space, it also cannot contain double quotation marks (").
all	Deletes all AP user-defined applications.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

If the specified AP user-defined application name does not exist, a new AP user-defined application is created and the AP user-defined application view is displayed. If the specified AP user-defined application name exists, the AP user-defined application view is directly displayed. If the **name** parameter is not specified, the user-defined application named **UD_id** is created by default.

Example

Create the AP user-defined application **UD_abc**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc]
```

11.9.26 user-protocol-statistic enable

Function

The **user-protocol-statistic enable** command enables the user protocol statistics collection function.

The **undo user-protocol-statistic enable** command disables the user protocol statistics collection function.

By default, the user protocol statistics collection function is disabled.

Format

user-protocol-statistic enable

undo user-protocol-statistic enable

Parameters

None

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

After going online on an AP, users start various applications on STAs to access the network. By analyzing packets sent by STAs, the collects information about network usage by applications of each user and reports the collected information (including the IP and MAC addresses of STAs and the application types) to the network management system (NMS). The NMS then displays and stores the information, which the administrator can view at any time. To identify user-based applications, run the **user-protocol-statistic enable** command.

NOTE

This function takes effect only for STAs who go online after the **user-protocol-statistic enable** command is successfully executed.

Example

Enable the user protocol statistics collection function in the SAC profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] user-protocol-statistic enable
```

11.9.27 vap-protocol-statistic enable

Function

The **vap-protocol-statistic enable** command enables the protocol statistics collection function in a VAP.

The **undo vap-protocol-statistic enable** command disables the protocol statistics collection function in a VAP.

By default, the protocol statistics collection function is disabled in a VAP.

Format

vap-protocol-statistic enable

undo vap-protocol-statistic enable

Parameters

None

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

After going online on an AP, users start various applications on STAs to access the network. By analyzing packets sent by STAs, the collects information about network usage by applications of each user and reports the collected information (including the IP and MAC addresses of STAs and the application types) to the network management system (NMS). The NMS then displays and stores the information, which the administrator can view at any time. To identify applications in a VAP, run the **vap-protocol-statistic enable** command.

Example

Enable the protocol statistics collection function for VAPs in SAC profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] vap-protocol-statistic enable
```

11.10 WLAN Location Configuration Commands

11.10.1 Command Support

- WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.
- The AeroScout MU location function is not supported by the following models:
  - AirEngine X760 series APs running V200R022C00 or earlier
  - AirEngine X761 series APs running V200R022C00 or earlier
  - AirEngine X762 series APs running V200R022C00 or earlier (In V200R022C10 and later versions, these APs support only single AP-based AeroScout MU location but do not support three-point location.)
  - AirEngine series central APs (including matching RUs) running V200R022C00 or earlier

  - AirEngine 9700D-S (including matching ORUs)
- The Wi-Fi tag location function is not supported by the following models:
  - AirEngine X760 series APs: do not support Ekahau tag location, and do not support AeroScout tag location in V200R022C00 or earlier.
  - AirEngine X761 series APs: do not support Ekahau tag location, and do not support AeroScout tag location in V200R022C00 or earlier.
  - AirEngine X771 series APs: do not support Ekahau tag location.
  - AirEngine X762 series APs
  - AirEngine series central APs (including matching RUs): do not support Ekahau tag location, and do not support AeroScout tag location in V200R022C00 or earlier.
  - AirEngine 9700D-S (including matching ORUs)
- Only the following models support Bluetooth terminal location, Bluetooth tag location, and Bluetooth data transparent transmission:
  - AirEngine X760 series APs
  - AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
  - AirEngine X771 series APs
  - AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later
- The Bluetooth broadcast function is supported only by the following models:
  - AirEngine X760 series APs
  - AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
  - AirEngine X771 series APs
  - AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

11.10.2 aeroscout compound-time

Function

The **aeroscout compound-time** command configures the aggregation time of AeroScout tag and mobile unit (MU) packets on the AC.

The **undo aeroscout compound-time** command restores the default aggregation time of AeroScout tag and MU packets.

The default aggregation time of AeroScout tag and MU packets is 6553.5s on the AC.

Format

aeroscout compound-time *time-value*

undo aeroscout compound-time

Parameters

Parameter	Description	Value
time-value	Specifies the packet aggregation time.	The value is an integer that ranges from 0 to 65535. The unit is in 0.1s. If *time-value* is set to 0, the AP does not aggregate packets but reports the packets in real time.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During AeroScout location, the AP does not report the received tag packets immediately to the upstream device but aggregates the packets. After a specified time, the AP reports the aggregated packets.

The AeroScout location server delivers an aggregation time of 6553.5s to the APs. The AC delivers the aggregation time to the APs using the **aeroscout compound-time** command. The AP selects a smaller aggregation time. By default, the aggregation time on the APs is 6553.5s.

If the packet aggregation time is set to a large value on the AeroScout location system, it takes a long time for the AP to report the aggregated packets, resulting in poor real-time performance and a large delay in the transmission of location packets. You can run the **aeroscout compound-time** command to set a small aggregation time to reduce the delay in location packet transmission.

Precautions

When the size of aggregated packets on an AP reaches 1k bytes, the AP immediately reports the aggregated packets.

Example

Set the aggregation time to 10s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] aeroscout compound-time 100
```


11.10.3 aeroscout local

Function

The **aeroscout local** command configures a local IP address used by the AC to receive packets from a location server.

The **undo aeroscout local** command deletes the configured local IP address used by the AC to receive packets from a location server.

By default, no local IP address is configured for the AC to receive packets from a location server.

Format

aeroscout local ip-address *ip-address*

undo aeroscout local

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies a local IPv4 address used by the AC to receive packets from a location server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **aeroscout server port** *port-num* **via-ac ac-port** *ac-port-num* command is executed to configure location data to be reported through the AC, run the **aeroscout local ip-address** *ip-address* command to configure a local IP address used by the AC to receive packets from a location server. The AC can receive packets from the location server only using this IP address.

Precautions

You need to run the **source ip-address** *ip-address* command to configure the source IP address used by the AC to send packets to the location server.

Example

Configure 10.1.1.1 as the local IP address used by the AC to receive packets from a location server.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] aeroscout local ip-address 10.1.1.1
```

11.10.4 aeroscout mu-enable

Function

The **aeroscout mu-enable** command enables WLAN location of AeroScout mobile units (MUs).

The **undo aeroscout mu-enable** command disables WLAN location of AeroScout MUs.

By default, WLAN location of AeroScout MUs is disabled.

Format

aeroscout mu-enable

undo aeroscout mu-enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **aeroscout mu-enable** command to enable WLAN location of AeroScout MUs.

Example

Enable WLAN location of AeroScout MUs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] aeroscout mu-enable
```

11.10.5 aeroscout server

Function

The **aeroscout server** command sets the port number for APs to report location packets of AeroScout tags and Mobile Units (MUs).

The **undo aeroscout server** command deletes the configured port number for APs to report location packets of AeroScout tags and MUs.

By default, no port number is configured for APs to report location packets of AeroScout tags and MUs.

Format

aeroscout server port *port-num* [**via-ac ac-port** *ac-port-num*]

undo aeroscout server

Parameters

Parameter	Description	Value
port *port-num*	Specifies a port number through which APs report location packets of AeroScout tags and MUs when APs are configured to directly report data. Specifies a port number through which the AC reports location packets of AeroScout tags and MUs when the AC is configured to forward data.	The value is an integer that ranges from 1025 to 65535.
via-ac	Indicates that the AC forwards location packets of AeroScout tags and MUs reported by APs to the AeroScout server. **NOTE** If the APs report the received tag packets and MU packets directly to the AeroScout location server, the **display wlan location statistics aeroscout** command cannot collect statistics about AeroScout tag locations and MU locations, and the **display wlan location config-info aeroscout** command cannot display the configuration delivered by the AeroScout location server to APs.	-
ac-port *ac-port-num*	Specifies the destination port number on the AC to which APs report location packets of AeroScout tags and MUs.	The value is an integer that ranges from 1025 to 65535.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Location packets of AeroScout tags and MUs received by APs can be reported to the AeroScout location server directly or through the AC.

Precautions

You cannot configure a port number that has been occupied by other services. Otherwise, the destination port configuration fails.

For the same location method, via-ac can be configured only in one profile. If **via-ac** has been specified in the current location profile for a specific location method, it cannot be specified in other profiles for the same location method.

NOTE

An AeroScout server proactively establishes connections with APs. Therefore, manually add the APs and specify their MAC addresses, port numbers, and IP addresses on the AeroScout server. If the AC is configured to forward location data, you only need to specify the AC IP address. You do not need to specify the IP address of the AeroScout server on the AC.

Follow-up Procedure

If the AC is configured to forward location packets to the location server, run the **source ip-address** *ip-address* command to configure the source IP address for the AC to send packets to the location server and run the **aeroscout local ip-address** *ip-address* command to configure a local IP address for the AC to receive packets from the location server.

Example

Set the port number for APs to report location packets of AeroScout tags and MUs to 1144.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] aeroscout server port 1144
```

11.10.6 aeroscout tag-enable

Function

The **aeroscout tag-enable** command enables WLAN location of AeroScout tags.

The **undo aeroscout tag-enable** command disables WLAN location of AeroScout tags.

By default, WLAN location of AeroScout tags is disabled.

Format

aeroscout tag-enable

undo aeroscout tag-enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **aeroscout tag-enable** command to enable WLAN location of AeroScout tags.

Example

Enable WLAN location of AeroScout tags.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] aeroscout tag-enable
```

11.10.7 ble low-power-threshold

Function

The **ble low-power-threshold** command sets a low power alarm threshold for BLE devices or Bluetooth tags.

The **undo ble low-power-threshold** command restores the low power alarm threshold of BLE devices or Bluetooth tags to the default value.

By default, the low power alarm threshold of BLE devices or Bluetooth tags is 20%.

Format

ble low-power-threshold *low-power-threshold*

undo ble low-power-threshold

Parameters

Parameter	Description	Value
low-power-threshold	Specifies the low power alarm threshold of BLE devices or Bluetooth tags.	The value is an enumerated type. The options are as follows: • 0: 0% • 20: 20% • 40: 40% • 60: 60% • 80: 80%

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After the **sniffer enable** command is executed to enable the Bluetooth monitoring or Bluetooth tag location function of an AP's built-in Bluetooth module, the built-in Bluetooth module will scan and obtain information about surrounding BLE devices or Bluetooth tags. The information includes battery power of BLE devices or Bluetooth tags. When the obtained battery power of a BLE device or Bluetooth tag is lower than the low power alarm threshold, the AC generates an alarm indicating that the BLE device or Bluetooth tag has low battery power.

Example

Set the low power alarm threshold for BLE devices or Bluetooth tags to 40%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble low-power-threshold 40
```

11.10.8 ble monitoring-list

Function

The **ble monitoring-list** command adds specified Bluetooth devices to the Bluetooth device monitoring list.

The **undo ble monitoring-list** command deletes specified Bluetooth devices from the Bluetooth device monitoring list.

By default, no Bluetooth devices are added to the monitoring list.

Format

ble monitoring-list { **all** | **mac** *mac-address1* [**to** *mac-address2*] }

undo ble monitoring-list { **all** | **mac** *mac-address1* [**to** *mac-address2*] }

Parameters

Parameter	Description	Value
mac *mac-address1*	Specifies the MAC address of a Bluetooth device to be monitored.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
to *mac-address2*	Specifies the end MAC address of a Bluetooth device when Bluetooth devices are added to or deleted from the monitoring list in batches. The *mac-address2* value must be greater than or equal to the *mac-address1* value. *mac-address1* and *mac-address2* together specify a range of MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
all	Indicates all Bluetooth devices.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Bluetooth monitoring, Bluetooth tag location, or Bluetooth data transparent transmission function is enabled using the **sniffer enable** command, no Bluetooth device is monitored when no Bluetooth device (BLE device, Bluetooth tag, or Bluetooth client) is added to the monitoring list. After Bluetooth devices are added to the monitoring list, only the Bluetooth devices in the list are monitored. When a Bluetooth device in the monitoring list is offline or has insufficient battery power, an alarm is triggered on the device accordingly. Bluetooth clients do not support low battery power alarms.

Precautions

After the Bluetooth monitoring, Bluetooth tag location, or Bluetooth data transparent transmission function is disabled using the **undo sniffer enable**

command, an alarm is triggered on the device, indicating that Bluetooth devices are offline.

Bluetooth devices with all-0 or all-F MAC addresses cannot be added to the monitoring list.

Example

Add the Bluetooth device with the MAC address 00e0-fc12-3456 to the monitoring list.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble monitoring-list mac 00e0-fc12-3456
```

Add the Bluetooth devices with MAC addresses from 00e0-fc12-3456 to 00e0-fc12-3458 to the monitoring list.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble monitoring-list mac 00e0-fc12-3456 to 00e0-fc12-3458
```

Disable the device from monitoring Bluetooth devices.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] undo ble monitoring-list all
Warning: This operation will delete all the manually configured Bluetooth monitoring lists. Continue? [Y/N]:y
```

11.10.9 ble report interval

Function

The **ble report interval** command sets an interval at which an AP reports Bluetooth device information.

The **undo ble report interval** command restores the default interval at which an AP reports Bluetooth device information.

By default, an AP reports Bluetooth device information at an interval of 10 minutes.

Format

ble report interval *interval-value*

undo ble report interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval at which an AP reports Bluetooth device information.	The value is an integer that ranges from 1 to 60, in minutes.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP collects information about 255 Bluetooth devices, the AP stops collecting information about more Bluetooth devices. When the aging time of Bluetooth device information collected by an AP expires, the AP clears aged device information and scans for new Bluetooth device information. The aging time of Bluetooth device information cannot be configured. The default aging time is 10 minutes. When the interval at which an AP reports Bluetooth device information times out, the AP reports Bluetooth device information to an AC. Bluetooth device information includes types, RSSIs, and whether Bluetooth tags are disconnected.

Example

Set the interval at which an AP reports Bluetooth device information to 20 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble report interval 20
```

11.10.10 ble source

Function

The **ble source** command configures a global source IP address in packets sent by an AC to a location server.

The **undo ble source** command deletes a global source IP address from packets sent by an AC to a location server.

By default, the source IP address is not configured in packets sent by an AC to a location server, and the IP address of the route outbound interface is used as the source IP address.

Format

ble source ip-address *ip-address*

undo ble source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies a source IPv4 address in packets sent by an AC to a location server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Bluetooth location scenarios, you can run the **ble source** command to configure a source IP address in packets sent by an AC to a location server.

Run the **ble source** command to configure different source IP addresses for the active and standby ACs.

When source IP addresses are configured on an AC using the **ble source** and **source** commands at the same time, the source IP address configured using the **source** command takes effect.

Precautions

- Ensure that the AC IP address manually configured on the location server is the same as that configured using the **ble source** command.
- The source IP address must exist on the AC; otherwise, the configuration does not take effect.

Example

Configure 10.102.25.23 as the source IP address of the packets sent from the AC to the location server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble source ip-address 10.102.25.23
```

11.10.11 ble-profile (AP group view and AP view)

Function

The **ble-profile** command binds a BLE profile to an AP group or AP.

The **undo ble-profile** command unbinds a BLE profile from an AP group or AP.

By default, no BLE profile is bound to an AP group or AP.

Format

ble-profile *profile-name*

undo ble-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a BLE profile.	The BLE profile name must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a BLE profile using the **ble-profile (WLAN view)** command, you need to bind the profile in the AP view or AP group view to make the settings in the profile take effect.

Precautions

After you bind a BLE profile in the AP view or AP group view, parameter settings in the BLE profile take effect for all APs using this profile.

Example

Create BLE profile **example** and bind the profile to AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] quit
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] ble-profile example
```

11.10.12 ble-profile (WLAN view)

Function

The **ble-profile** command creates a BLE profile or displays the BLE profile view.

The **undo ble-profile** command deletes a BLE profile.

By default, no BLE profile is created.

Format

ble-profile name *profile-name*

undo ble-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a BLE profile, which must be unique and identifies a profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all BLE profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to create or delete a BLE profile or enter the BLE profile view to configure the profile. If the specified profile name does not exist, this command creates a new BLE profile and displays the configuration view of this profile. All parameters in this profile use default values. You can also change values of these parameters.

Follow-up Procedure

After creating a BLE profile, you need to run the **ble-profile (AP group view and AP view)** command in the AP view or AP group view to bind the profile to make the settings in the profile take effect.

Precautions

A BLE profile bound to an AP or AP group cannot be deleted. To delete a BLE profile, unbind it in the AP view or AP group view.

Example

Create BLE profile **example** and enter its view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example]
```

11.10.13 broadcaster enable

Function

The **broadcaster enable** command enables the Bluetooth broadcast function of an AP's built-in Bluetooth module.

The **undo broadcaster enable** command disables the Bluetooth broadcast function of an AP's built-in Bluetooth module.

By default, the Bluetooth broadcast function of an AP's built-in Bluetooth module is disabled.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcaster enable

undo broadcaster enable

Parameters

None

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

When an AP's built-in Bluetooth module is used as a BLE device, you can run this command to enable the Bluetooth broadcast function. After this function is enabled, the built-in Bluetooth module sends BLE broadcast frames to surrounding devices. The frame content complies with the iBeacon protocol.

Enabling both the Bluetooth scanning and broadcast functions of an AP affects the efficiency for the AP's Bluetooth module to scan surrounding BLE devices. When an AP does not serve as a Bluetooth base station, it is recommended that the broadcast function of the AP be disabled.

Example

Enable the Bluetooth broadcast function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] broadcaster enable
```

11.10.14 broadcasting-content

Function

The **broadcasting-content** command configures the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

The **undo broadcasting-content** command restores the default content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

By default, the UUID, Major, and Minor fields in a BLE broadcast frame sent by an AP's built-in Bluetooth module are null, and the RSSI calibration value is –65 dBm.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcasting-content { **uuid** { **uuid-character-string** *uuid-value* | **uuid-hex** *uuid-value* } | **major** { **major-character-string** *major-value* | **major-hex** *major-value* | **major-decimal** *major-value* } | **minor** { **minor-character-string** *minor-value* | **minor-hex** *minor-value* | **minor-decimal** *minor-value* } | **reference-rssi** *reference-rssi-value* }*

undo broadcasting-content [**uuid** | **major** | **minor** | **reference-rssi**]

Parameters

Parameter	Description	Value
uuid uuid-character-string *uuid-value*	Specifies the UUID field in a BLE broadcast frame. UUID is the universally unique identifier of a BLE device.	The value is a string of 1 to 16 characters. The default value is null.
uuid uuid-hex *uuid-value*	Specifies the UUID field in a BLE broadcast frame. UUID is the universally unique identifier of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 32 bytes. The default value is null.
major major-character-string *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.
major major-hex *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 4 bytes. The default value is null.
major major-decimal *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is an integer that ranges from 0 to 65535. The default value is null.
minor minor-character-string *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.

Parameter	Description	Value
minor minor-hex *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 4 bytes. The default value is null.
minor minor-decimal *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is an integer that ranges from 0 to 65535. The default value is null.
reference-rssi *reference-rssi-value*	Specifies the RSSI calibration value of a BLE device. RSSI calibration value indicates the RSSI value of a BLE device measured at a distance of 1 m. It is used to estimate the distance between the BLE device and Bluetooth terminals.	The value is an integer that ranges from –97 to –50, in dBm. The default value is -65 that is measured when the transmit power of an APs' built-in Bluetooth module is 0 dBm.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the broadcast function of an AP's built-in Bluetooth module using the **broadcaster enable** command, you can run this command to configure the content of BLE broadcast frames sent by the module.

Precautions

The RSSI calibration value in a BLE broadcast frame is set based on the actual measurement result.

After changing the transmit power of a built-in Bluetooth module using the **tx-power (BLE profile view)** command, you need to measure and configure the RSSI calibration value again. Therefore, you are advised to run the **tx-power (BLE profile view)** command to configure the transmit power of a built-in Bluetooth module before configuring the RSSI calibration value.

Example

Configure the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module. Set **UUID uuid-hex** to **12345678123456789**, **Major major-hex** to **A22**, **Minor minor-hex** to **011**, and **reference-rssi** to **-70**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] broadcasting-content uuid uuid-hex 12345678123456789 major major-hex A22 minor minor-hex 011 reference-rssi -70
```

Configure the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module. Set **LocalName** to **name1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] broadcasting-content local-name name1
```

11.10.15 broadcasting-content (AP group view)

Function

The **broadcasting-content** command configures the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

The **undo broadcasting-content** command restores the default content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

By default, the UUID of the BLE broadcast frames sent by an AP's built-in Bluetooth module is null.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcasting-content uuid { **uuid-character-string** *uuid-value* | **uuid-hex** *uuid-value* }

undo broadcasting-content uuid

Parameters

Parameter	Description	Value
uuid uuid-character-string *uuid-value*	Specifies the UUID field of BLE broadcast frames, which is a string of characters and used to identity devices.	The value is a string of 1 to 16 characters.
uuid uuid-hex *uuid-value*	Specifies the UUID field of BLE broadcast frames, which is in hexadecimal notation and used to identity devices.	The value is a string of 1 to 32 hexadecimal characters.

Views

AP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the broadcast function of an AP's built-in Bluetooth module using the **broadcaster enable** command, you can run this command to configure the UUID of BLE broadcast frames sent by the module.

Precautions

The UUIDs set in the AP view, BLE profile bound to the AP view, AP group view, and BLE profile bound to the AP group take effect in the following order:

1. UUID set in the AP view
2. UUID set in the BLE profile bound to the AP view
3. UUID set in the AP group view
4. UUID set in the BLE profile bound to the AP group view

Example

Set the UUID of the BLE broadcast frames sent by an AP's Bluetooth module in the AP group view to **12345678123456789** in hexadecimal notation.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name mygroup
[HUAWEI-wlan-ap-group-mygroup] broadcasting-content uuid uuid-hex 12345678123456789
```

11.10.16 broadcasting-content (AP view)

Function

The **broadcasting-content** command configures the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

The **undo broadcasting-content** command restores the default content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

By default, the UUID, Major, Minor, and RSSI calibration fields in a BLE broadcast frame sent by an AP's built-in Bluetooth module are null.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcasting-content { **uuid** { **uuid-character-string** *uuid-value* | **uuid-hex** *uuid-value* } | **major** { **major-character-string** *major-value* | **major-hex** *major-value* | **major-decimal** *major-value* } | **minor** { **minor-character-string** *minor-value* | **minor-hex** *minor-value* | **minor-decimal** *minor-value* } | **reference-rssi** *reference-rssi-value* }*

undo broadcasting-content [**uuid** | **major** | **minor** | **reference-rssi**]

Parameters

Parameter	Description	Value
uuid uuid-character-string *uuid-value*	Specifies the UUID field of BLE broadcast frames, which is a string of characters and used to identity devices.	The value is a string of 1 to 16 characters.
uuid uuid-hex *uuid-value*	Specifies the UUID field of BLE broadcast frames, which is in hexadecimal notation and used to identity devices.	The value is a string of 1 to 32 hexadecimal characters.
major major-character-string *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.

Parameter	Description	Value
major major-hex *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 4 bytes. The default value is null.
major major-decimal *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is an integer that ranges from 0 to 65535. The default value is null.
minor minor-character-string *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.
minor minor-hex *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 4 bytes. The default value is null.
minor minor-decimal *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is an integer that ranges from 0 to 65535. The default value is null.
reference-rssi *reference-rssi-value*	Specifies the RSSI calibration value of a BLE device. RSSI calibration value indicates the RSSI value of a BLE device measured at a distance of 1 m. It is used to estimate the distance between the BLE device and Bluetooth terminals.	The value is an integer that ranges from –97 to –50, in dBm. The default value is null.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the broadcast function of an AP's built-in Bluetooth module using the **broadcaster enable** command, you can run this command to configure the content of BLE broadcast frames sent by the module.

Precautions

The contents set in the AP view, BLE profile bound to the AP view, AP group view, and BLE profile bound to the AP group take effect in the following order:

1. Contents set in the AP view
2. Contents set in the BLE profile bound to the AP view
3. Contents set in the AP group view
4. Contents set in the BLE profile bound to the AP group view

Example

Set the UUID of the BLE broadcast frames sent by an AP's Bluetooth module in the AP view to **12345678123456789** in hexadecimal notation.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] broadcasting-content uuid uuid-hex 12345678123456789
```

11.10.17 broadcasting-interval

Function

The **broadcasting-interval** command configures the interval for an AP's built-in Bluetooth module to send BLE broadcast frames.

The **undo broadcasting-interval** command restores the default interval for an AP's built-in Bluetooth module to send BLE broadcast frames.

By default, the built-in Bluetooth module of an AP sends BLE broadcast frames at an interval of 500 ms.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcasting-interval *broadcasting-interval-value*

undo broadcasting-interval

Parameters

Parameter	Description	Value
broadcasting-interval-value	Specifies the interval for an AP's built-in Bluetooth module to send BLE broadcast frames.	The value is an integer that ranges from 100 to 10240, in milliseconds.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

After enabling the broadcast function of an AP's built-in Bluetooth module using the **broadcaster enable** command, you can run this command to set the interval for the module to send BLE broadcast frames.

Example

Set the interval for an AP's built-in Bluetooth module to send BLE broadcast frames to 1000 ms.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] broadcasting-interval 1000
```

11.10.18 display ble-profile

Function

The **display ble-profile** command displays configuration and reference information about a BLE profile.

Format

display ble-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all BLE profiles.	-
name *profile-name*	Displays information about the BLE profile with a specified name.	The BLE profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about BLE profiles.

Example

Display information about all BLE profiles.

```
<HUAWEI> display ble-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
example                         1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-197 Description of the **display ble-profile all** command output

Item	Description
Profile name	BLE profile name.
Reference	Number of times a BLE profile is referenced.

Display information about the BLE profile **example**.

```
<HUAWEI> display ble-profile name example
--------------------------------------------------------------------------------
Broadcaster switch           : disable
Broadcaster interval(ms)     : 500
Broadcaster content
  UUID                       : 00000000000000012345678123456789(hex)
  Major                      : 0A22(hex)
  Minor                      : 0011(hex)
  Reference RSSI             : -70
```



```
Transmit power              : 0
Sniffer switch             : disable
Sniffer mode               : -
Source IP address           : 0.0.0.0
Report switch              : enable
Report mode                 : immediate
Report interval(s)         : 10
Report server              : 0.0.0.0
Report server port          : -
Report via-AC              : disable
Report via-AC port          : -
------------------------------------------------------------------------------
```

Table 11-198 Description of the **display ble-profile name** *profile-name* command output

Item	Description
Broadcaster switch	Whether the Bluetooth broadcast function is enabled. • enable • disable To configure this parameter, run the **broadcaster enable** command.
Broadcaster interval(ms)	Interval at which BLE broadcast frames are sent. To configure this parameter, run the **broadcasting-interval** command.
Broadcaster content	Content of a BLE broadcast frame. To configure this parameter, run the **broadcasting-content** command.
UUID	UUID field in a BLE broadcast frame. UUID refers to the universally unique identifier of a Bluetooth device.
Major	Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of the BLE device.
Minor	Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of the BLE device.

Item	Description
Reference RSSI	RSSI calibration value. This value refers to the RSSI of a BLE device measured at a distance of 1 m. It is used to calculate the distance between a BLE device and a BLE terminal or tag.
MQTT Server	MQTT server configuration. To configure this parameter, run the **mqtt-server** command.
Transmit power	Transmit power of an AP's built-in Bluetooth module. To configure this parameter, run the **tx-power (BLE profile view)** command.
Sniffer switch	Whether the Bluetooth function is enabled. ● enable ● disable To configure this parameter, run the **sniffer enable** command.
Sniffer mode	Bluetooth working mode. To configure this parameter, run the **sniffer enable** command.
Source IP address	Source IP address used to report Bluetooth packets. To configure this parameter, run the **source (BLE profile view)** command.
Report switch	Whether Bluetooth packets are reported. ● enable ● disable To configure this parameter, run the **report enable** command.
Report mode	Mode in which an AP reports Bluetooth packets. To configure this parameter, run the **report-mode** command.
Report interval(s)	Interval at which an AP reports Bluetooth packets. To configure this parameter, run the **report-mode** command.

Item	Description
Report server	IP address of a Bluetooth server. To configure this parameter, run the **report-to-server** command.
Report server port	Port number of a Bluetooth server. To configure this parameter, run the **report-to-server** command.
Report via-AC	Whether Bluetooth packets are reported to a server through the AC. • enable: Bluetooth packets are reported through the AC. • disable: Bluetooth packets are reported not through the AC. To configure this parameter, run the **report-to-server** command.
Report via-AC port	Port number used by the AC to report Bluetooth packets. To configure this parameter, run the **report-to-server** command.

11.10.19 display location-profile

Function

The **display location-profile** command displays configuration information about a location profile.

Format

display location-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Specifies all location profiles.	-
name *profile-name*	Specifies a location profile.	The location profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration information about a location profile to verify the configuration.

Example

Display all location profiles.

```
<HUAWEI> display location-profile all
-------------------------------------------------------------
Profile name                Reference
-------------------------------------------------------------
default                      1
-------------------------------------------------------------
Total: 1
```

Table 11-199 Description of the **display location-profile all** command output

Item	Description
Profile name	Name of a location profile.
Reference	Number of times a location profile is referenced.

Display the default configuration of the location profile **default**.

```
<HUAWEI> display location-profile name default
-------------------------------------------------------------------------------
Aeroscout-tag                 : disable
Aeroscout-mu                  : disable
Aeroscout ae-port             : -
Aeroscout compound-time(100ms) : 65535
Aeroscout via-AC              : disable
Aeroscout via-AC port         : -
Ekahau-tag                    : disable
Ekahau erc IP-address         : 0.0.0.0
Ekahau erc port               : -
Ekahau via-AC                 : disable
Ekahau via-AC port            : -
Source IP-address             : 0.0.0.0
private mu                    : disable
private server                : 0.0.0.0
private server domain         : -
private server port           : -
private via-AC                : disable
private via-AC port           : -
private report-frequency(ms)   : 20000
private report-protocol       : udp
private ssl-policy name       : -
private mu protocol-version    : v3
collect location data                 : disable
collect location data RSSI threshold(dBm)  : -75
-------------------------------------------------------------
```


Table 11-200 Description of the **display location-profile name default** command output

Item	Description
Aeroscout-tag	Whether WLAN location of AeroScout tags is enabled. To configure this parameter, run the **aeroscout tag-enable** command.
Aeroscout-mu	Whether WLAN location of AeroScout MUs is enabled. To configure this parameter, run the **aeroscout mu-enable** command.
Aeroscout ae-port	Port number used by APs to report location packets. To configure this parameter, run the **aeroscout server** command.
Aeroscout compound-time	Aggregation time of AeroScout location packets. To configure this parameter, run the **aeroscout compound-time** command.
Aeroscout via-AC	Whether AeroScout location packets are reported to the location server through an AC. ● enable: The AeroScout location packets are reported to the location server through an AC. ● disable: The AeroScout location packets are not reported to the location server through an AC. To configure this parameter, run the **aeroscout server** command.
Aeroscout via-AC port	Port number used by an AC to report AeroScout location packets. To configure this parameter, run the **aeroscout server** command.
Ekahau-tag	Whether WLAN location of Ekahau tags is enabled. To configure this parameter, run the **ekahau tag-enable** command.
Ekahau erc IP-address	IP address of the Ekahau location server. To configure this parameter, run the **ekahau server** command.

Item	Description
Ekahau erc port	Port number of the Ekahau location server. To configure this parameter, run the **ekahau server** command.
Ekahau via-AC	Whether Ekahau location packets are reported to the location server through an AC. • enable: The Ekahau location packets are reported to the location server through an AC. • disable: The Ekahau location packets are not reported to the location server through an AC. To configure this parameter, run the **ekahau server** command.
Ekahau via-AC port	Port number used by an AC to report Ekahau location packets. To configure this parameter, run the **ekahau server** command.
Source IP-address	Source IP address used by an AC to report location packets. To configure this parameter, run the **source (location profile view)** command.
private mu	Whether terminal location is enabled. To configure this parameter, run the **private mu-enable** command.
private server	IP address of the terminal location server. To configure this parameter, run the **private server** command.
private server domain	Domain name of the terminal location server. To configure this parameter, run the **private server** command.
private server port	Port number of the terminal location server. To configure this parameter, run the **private server** command.

Item	Description
private via-AC	Whether terminal location packets are reported to the location server through an AC. • enable: The terminal location packets are reported to the location server through an AC. • disable: The terminal location packets are not reported to the location server through an AC. To configure this parameter, run the **private server** command.
private via-AC port	Port number used by an AC to report terminal location packets. To configure this parameter, run the **private server** command.
private report-frequency(ms)	Interval at which an AP reports terminal location packets. To configure this parameter, run the **private report-frequency** command.
private report-protocol	Protocol used by an AP to report information. To configure this parameter, run the **private report-protocol** command.
private ssl-policy name	SSL policy used when the terminal location protocol is HTTPS. To configure this parameter, run the **private report-protocol** command.
private mu protocol-version	Terminal location protocol version. To configure this parameter, run the **private mu protocol-version** command.
collect location data	Whether the device is enabled to collect wireless device location data. To configure this parameter, run the **collect-location-data enable** command.
collect location data RSSI threshold(dBm)	RSSI threshold for wireless device location data. To configure this parameter, run the **collect-location-data rssi-threshold** command.

11.10.20 display references ble-profile

Function

The **display references ble-profile** command displays reference information about a BLE profile.

Format

display references ble-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified BLE profile.	The BLE profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view reference information about a BLE profile.

Example

Display reference information about BLE profile **example**.

```
<HUAWEI> display references ble-profile name example
------------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------------
AP group                    default
------------------------------------------------------------------------------
Total: 1
```

Table 11-201 Description of the **display references ble-profile** command output

Item	Description
Reference type	Type of the profile that references a BLE profile.
Reference name	Name of the profile that references a BLE profile.

11.10.21 display wlan ble global configuration

Function

The **display wlan ble global configuration** command displays global configurations of Bluetooth devices.

Format

display wlan ble global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view global configurations of Bluetooth devices and know the configuration about the Bluetooth device information report function.

Example

Display global configurations of Bluetooth devices.

```
<HUAWEI> display wlan ble global configuration
------------------------------------------------------------------------------
BLE report interval(min)       :10
BLE low power threshold(%)     :20
BLE source IP address          :0.0.0.0
------------------------------------------------------------------------------
```

Table 11-202 Description of the **display wlan ble global configuration** command output

Item	Description
BLE report interval(min)	Interval at which an AP reports Bluetooth device information.
BLE low power threshold(%)	Low power alarm threshold of Bluetooth devices.
BLE source IP address	A global source IP address in packets sent by an AC to a location server.

11.10.22 display wlan ble monitoring-list

Function

The **display wlan ble monitoring-list** command displays the BLE device monitoring list.

Format

display wlan ble monitoring-list

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **ble monitoring-list mac** command to add BLE devices to the monitoring list, you can run the **display wlan ble monitoring-list** command to check BLE devices in the monitoring list.

If you run the **ble monitoring-list all** command to monitor all BLE devices, you can run the **display wlan ble monitoring-list** command to check BLE devices scanned by APs.

Example

Display the BLE device monitoring list.

```
<HUAWEI> display wlan ble monitoring-list
--------------------------------------------------------------------------------
Index       MAC
--------------------------------------------------------------------------------
0           00e0-fc34-0000
1           00e0-fc34-7777
--------------------------------------------------------------------------------
Total: 2
```

Table 11-203 Description of the **display wlan ble monitoring-list** command output

Item	Description
Index	Index.
MAC	MAC address of a BLE device.

11.10.23 display wlan ble site-info

Function

The **display wlan ble site-info** command displays information about Bluetooth devices that are scanned by an AP's built-in Bluetooth module.

Format

display wlan ble site-info { **all** | **mac-address** *mac-address* | **host-ap** { **valid** | **host-ap-id** *ap-id* | **host-ap-name** *ap-name* } }

Parameters

Parameter	Description	Value
all	Displays information about all Bluetooth devices.	-
mac-address *mac-address*	Displays information about a specified Bluetooth device.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
host-ap valid	Displays information about APs' built-in Bluetooth modules among all Bluetooth device information.	-
host-ap host-ap-id *ap-id*	Displays information about the Bluetooth module built in an AP with the specified ID.	The AP ID must exist.
host-ap host-ap-name *ap-name*	Displays information about the Bluetooth module built in an AP with the specified name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you enable the Bluetooth monitoring function using the **sniffer enable** command, an AP's built-in Bluetooth module scans surrounding Bluetooth devices

and obtains their information. You can then run this command to view obtained information about Bluetooth devices scanned by the built-in Bluetooth module.

After the Bluetooth broadcast function is enabled for an AP with the built-in Bluetooth module, the Bluetooth module works as a Bluetooth station, whose information can be found in Bluetooth device information. If the Bluetooth MAC address label of an AP is lost, it is time-consuming to locate the mapping between the AP and built-in Bluetooth module. In this case, configure the **host-ap** parameter to filter out information about the AP's built-in Bluetooth module among all Bluetooth device information.

Example

Display information about all Bluetooth devices.

```
<HUAWEI> display wlan ble site-info all
-------------------------------------------------------------------------------------------------------------------------------------
---------------------
Index  MAC             Host AP ID Host AP name RSSI  Power Type       DetachedFlag Aging-Timeout(m)
Broadcast count Advertisement data
-------------------------------------------------------------------------------------------------------------------------------------
---------------------
0      0000-0101-0202  4          AP4         -30   50%   asset-tag  N            57              10
02-02-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-fa
-------------------------------------------------------------------------------------------------------------------------------------
---------------------
Total: 1
```

Table 11-204 Description of the **display wlan ble site-info** command output

Item	Description
Index	Index.
MAC	MAC address of a Bluetooth device.
Host AP ID	ID of the AP to which a Bluetooth device belongs. The display of -- indicates that Bluetooth device information does not belong to the built-in Bluetooth module of the AP.
Host AP name	Name of the AP to which a Bluetooth device belongs. The display of -- indicates that Bluetooth device information does not belong to the built-in Bluetooth module of the AP.
RSSI	Signal strength of a Bluetooth device received by an AP's built-in Bluetooth module.
Power	Battery power of a Bluetooth device. If no information about battery power is obtained, this item is displayed as --.

Item	Description
Type	Bluetooth device type. The options are as follows: ● ibeacon: Bluetooth terminal ● asset-tag: Bluetooth tag ● sensor-tag: Bluetooth client
DetachedFlag	Whether a Bluetooth device is disconnected. The options are as follows: ● Y: The Bluetooth device is disconnected. ● N: The Bluetooth device is connected. **NOTE** Bluetooth device disconnection check is not supported in Bluetooth monitoring or transparent transmission mode. This parameter is valid only when the Bluetooth device type is **asset-tag**.
Aging-Timeout(m)	Remaining aging time of a Bluetooth device. The maximum value is 60 minutes.
Broadcast count	Number of broadcast packets sent by a Bluetooth device.
Advertisement data	Content of data carried in a broadcast frame sent by a Bluetooth device. The maximum length of a displayed broadcast frame is 21 bytes.

11.10.24 display wlan location config-info aeroscout

Function

The **display wlan location config-info aeroscout** command displays configurations delivered to APs from the AeroScout location server.

Format

display wlan location config-info aeroscout { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays the LBS configuration of the AP with a specified AP ID.	The AP ID must already exist.
ap-name *ap-name*	Displays the LBS configuration of the AP with a specified AP name.	The AP name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check configurations delivered to APs from the AeroScout location server.

Prerequisites

The AeroScout location function has been enabled using the **aeroscout tag-enable** or **aeroscout mu-enable** command, the AC has been enabled to forward location packets of AeroScout tags and MUs reported by APs to the AeroScout location server, and the AeroScout location server has delivered configuration information to the APs.

If the prerequisites are not met, for example, APs directly report packets of AeroScout tags and MUs to the AeroScout location server, a hyphen (-) is displayed after this command is run.

Example

Display AeroScout location configuration on the AP named **ap_4**.

```
<HUAWEI> display wlan location config-info aeroscout ap-name ap_4
------------------------------------------------------------------
AP ID                          : 4
AP name                        : ap_4
AP MAC address                 : 00e0-fc54-5a80
Response IP address            : 10.3.3.3
Response port                  : 1144
AP tag mode                    : start
AP MU mode                     : start
Dilution factor                : 100
Dilution timeout(s)            : 5
Tags multicast address         : 010c-cc00-0000
Compounded message timeout(0.1s) : 12
```


Table 11-205 Description of the **display wlan location config-info aeroscout** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
AP MAC address	AP's MAC address.
Response IP address	IP address of the location server used to receive the Response packets from the AP.
Response port	Port number used by APs to report location information.
AP tag mode	Tag detection status on the AP: ● start: The AP starts tag detection. ● stop: The AP stops tag detection. **NOTE** **AP tag mode** is displayed as **start** only when **aeroscout tag-enable** is configured on the AC and tag location is configured on the AeroScout location server.
AP MU mode	MU detection status on the AP: ● start: The AP starts MU detection. ● stop: The AP stops MU detection. **NOTE** **AP MU mode** is displayed as **start** only when **aeroscout mu-enable** is configured on the AC and MU location is configured on the AeroScout location server.
Dilution factor	Count-based packet dilution. For example, the value 100 indicates that one out of 100 packets is reported.
Dilution timeout(s)	Time-based packet dilution. For example, the value 1 indicates that at least one packet is reported every second.
Tags multicast address	Multicast MAC address of the tag.
Compounded message timeout(0.1s)	Maximum time during which the AP caches tag, in the unit of 100 milliseconds.

11.10.25 display wlan location device-info tag

Function

The **display wlan location device-info tag** command displays tag location information about APs.

Format

display wlan location device-info tag { **all** | **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
all	Displays tag location information about all APs.	-
ap-id *ap-id*	Displays tag location information about a specified AP ID.	The AP ID must exist.
ap-name *ap-name*	Displays tag location information about a specified AP name.	The AP name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view tag location information about APs, facilitating tag location statistics collection.

Example

Display tag location information about all APs.

```
<HUAWEI> display wlan location device-info tag all
AP ID   AP name     Tag type        Tag MAC          Channel     RSSI
------------------------------------------------------------------------------
0       ap1         AeroScout       00e0-fc76-e360   11          -50
1       ap3         Ekahau          00e0-fc76-e380   11          -50
------------------------------------------------------------------------------
Total: 2
```


Table 11-206 Description of the display wlan location device-info tag command output

Item	Description
AP ID	AP ID.
AP name	AP name.
Tag type	Type of the tag. The value is of the enumerated type. • Ekahau: Ekahau tag • AeroScout: AeroScout tag
Tag MAC	MAC address of the located tag.
Channel	Working channel of the located tag.
RSSI	RSSI of the located tag, in dBm.

11.10.26 display wlan location global configuration

Function

The **display wlan location global configuration** command displays global configurations of Wi-Fi location.

Format

display wlan location global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view global configurations of Wi-Fi location to learn about the configuration of reporting Wi-Fi location information.

Example

Display global configurations of Wi-Fi location.


```
<HUAWEI> display wlan location global configuration
------------------------------------------------------------------------------
Location source IP address     :0.0.0.0
Aeroscout local IP address     :-
------------------------------------------------------------------------------
```

Table 11-207 Description of the **display wlan location global configuration** command output

Item	Description
Location source IP address	Source IP address in location packets forwarded by the AC to the location server.
Aeroscout local IP address	Local IP address used by the AC to receive packets from the location server.

11.10.27 ekahau server

Function

The **ekahau server** command sets the destination IP address and port number for APs to report Ekahau tag location packets.

The **undo ekahau server** command deletes the configured destination IP address and port number for APs to report Ekahau tag location packets.

By default, no destination IP address or port number is configured for APs to report Ekahau tag location packets.

Format

ekahau server ip-address *ip-address* **port** *port-num* [**via-ac ac-port** *ac-port-num*]

undo ekahau server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IPv4 address of the Ekahau location server.	The value is in dotted decimal notation.

Parameter	Description	Value
port *port-num*	Specifies the destination port number on the Ekahau location server to which APs directly report Ekahau tag location packets. Specifies the destination port number on the Ekahau location server to which APs report Ekahau tag location packets through an AC.	The value is an integer that ranges from 1025 to 65535.
via-ac	Specifies that the Ekahau tag location packets received by APs are reported to the Ekahau location server through an AC.	-
ac-port *ac-port-num*	Specifies the destination port number on the AC to which APs report Ekahau tag location packets.	The value is an integer that ranges from 1025 to 65535.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Ekahau tag location packets received by APs can be reported to the Ekahau location server directly or through an AC.

Precautions

You cannot configure a port number that has been occupied by other services; otherwise, the port configuration fails.

For the same location method, via-ac can be configured only in one profile. If **via-ac** has been specified in the current location profile for a specific location method, it cannot be specified in other profiles for the same location method.

Example

Set the destination IP address and port number on the location server to which APs report Ekahau tag location packets to **192.168.1.2** and **8569**, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] ekahau server ip-address 192.168.1.2 port 8569
```


11.10.28 ekahau tag-enable

Function

The **ekahau tag-enable** command enables WLAN location of Ekahau tags.

The **undo ekahau tag-enable** command disables WLAN location of Ekahau tags.

By default, WLAN location of Ekahau tags is disabled.

Format

ekahau tag-enable

undo ekahau tag-enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ekahau tag-enable** command to enable WLAN location of Ekahau tags.

Example

Enable WLAN location of Ekahau tags.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] ekahau tag-enable
```

11.10.29 location source

Function

The **location source** command configures a global source IP address in packets sent by an AC to a location server.

The **undo location source** command deletes a global source IP address from packets sent by an AC to a location server.

By default, the source IP address is not configured in packets sent by an AC to a location server.

Format

location source ip-address *ip-address*

undo location source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies a source IPv4 address in packets sent by an AC to a location server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **location source** command to configure a source IP address in UDP packets sent by an AC to a location server.

Run the **location source** command to configure different source IP addresses for the active and standby ACs.

When source IP addresses are configured on an AC using the **location source** and **source** commands at the same time, the source IP address configured using the **source** command takes effect.

Precautions

- Ensure that the AC IP address manually configured on the location server is the same as that configured using the **location source** command.
- The source IP address must exist on the AC; otherwise, the configuration does not take effect.
- The source IP address in packets sent by an AC to a location server can be a global source IP address in the WLAN view and the source IP address in the location profile. The source IP address in the location profile takes precedence over the global source IP address in the WLAN view. If the source IP address in packets sent by an AC to a location server is not configured or the source IP address version is different from the IP address version of the location server, the AC's default IP address used for communicating with the location server is used as the source IP address.

Example

Configure 10.102.25.23 as the source IP address of the UDP packets sent from the AC to the location server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location source ip-address 10.102.25.23
```

11.10.30 location-profile

Function

The **location-profile** command binds a location profile to an AP radio.

The **undo location-profile** command unbinds a location profile from an AP radio.

By default, no location profile is bound to a radio.

Format

location-profile *profile-name* **radio** { *radio-id* | **all** }

undo location-profile radio { *radio-id* | **all** }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a location profile.	The location profile name must already exist.

Parameter	Description	Value
radio *radio-id*	Specifies the ID of the radio to which the location profile is bound.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: • AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 • AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T • AirEngine 8771-X1T
all	Binds the location profile to all radios.	-

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to bind a location profile to an AP group radio or AP radio. After the binding, the parameters of the location profile will be applied to the AP group radio or AP radio.

Example

Bind the location profile **default** to radio 0 of the AP group **ap-group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] location-profile default radio 0
```


11.10.31 location-profile (WLAN view)

Function

The **location-profile** command creates a location profile or displays the location profile view.

The **undo location-profile** command deletes a location profile.

By default, no location profile is created.

Format

location-profile name *profile-name*

undo location-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a location profile, which uniquely identifies a location profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all location profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

This command creates or deletes a location profile, or displays the location profile view in which you can configure the profile. If the specified profile name does not exist, the command creates a location profile and displays the view of this location profile, and all parameters in the location profile use default values. You can also change values of these parameters.

Example

Create the location profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name test
[HUAWEI-wlan-location-prof-test]
```

11.10.32 private mu protocol-version

Function

The **private mu protocol-version** command sets the terminal location protocol version.

The **undo private mu protocol-version** command restores the default terminal location protocol version.

The default terminal location protocol version is v3.

Format

private mu protocol-version { **v3** | **v5** }

undo private mu protocol-version

Parameters

Parameter	Description	Value
v3	Sets the protocol version to v3.	-
v5	Sets the protocol version to v5.	-

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the terminal location protocol version is v5, APs report more information to the location server, such as the timestamp (the time when APs scan STAs). The location server obtains the information to improve location accuracy.

Precautions

The terminal location protocol version must be the supported by the location server.

Example

Set the terminal location protocol version to v5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private mu protocol-version v5
```

11.10.33 private mu-enable

Function

The **private mu-enable** command enables terminal location of APs.

The **undo private mu-enable** command disables terminal location of APs.

By default, terminal location of APs is disabled.

Format

private mu-enable

undo private mu-enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **private mu-enable** command to enable terminal location of APs.

Example

Enable terminal location of APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private mu-enable
```

11.10.34 private report-frequency

Function

The **private report-frequency** command sets the interval at which an AP reports channel scan information.

The **undo private report-frequency** command restores the default interval at which an AP reports channel scan information.

By default, an AP reports channel scan information every 20000 ms.

Format

private report-frequency *time*

undo private report-frequency

Parameters

Parameter	Description	Value
time	Specifies the interval at which an AP reports channel scan information.	The value is an integer that ranges from 500 ms to 60000 ms.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

During terminal location, an AP periodically scans channels to collect data. The collected data is buffered and updated on the AP, then reported to the location server at specified intervals.

Example

Set the interval at which an AP reports channel scan information to 30000 ms.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private report-frequency 30000
```

11.10.35 private report-protocol

Function

The **private report-protocol** command sets a protocol type for APs to report information.

The **undo private report-protocol** command restores the default protocol type used by APs to report information.

By default, an AP uses UDP to reports information.

Format

private report-protocol { **udp** | **http** | **https ssl-policy** *ssl-policy* }

undo private report-protocol

Parameters

Parameter	Description	Value
udp	Sets the protocol type to UDP.	-
http	Sets the protocol type to HTTP.	-
https	Sets the protocol type to HTTPS.	-
ssl-policy *ssl-policy*	Specifies the name of an SSL policy.	The value is a string of 1 to 31 case-sensitive characters without spaces or question marks (**?**).

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If APs are used to report location data to a server, the protocol type can be set only to UDP.

If location data is reported to a server through the AC, the protocol type can be set to HTTP or UDP. If higher security is required, HTTPS is applicable.

Prerequisites

When the protocol type is set to HTTPS, an SSL policy must have been created and the AP has been configured to report terminal location information through an AC.

Example

Set the protocol type to HTTP for APs to report information.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private report-protocol http
```


Set the protocol type to HTTPS for APs to report information.
<HUAWEI> **system-view**
[HUAWEI] **wlan**
[HUAWEI-wlan-view] **location-profile name example**
[HUAWEI-wlan-location-prof-example] **private report-protocol https ssl-policy policy1**

11.10.36 private server

Function

The **private server** command configures the destination IP address and port number for APs to report STA location data.

The **undo private server** command restores the default destination IP address and port number for APs to report STA location data.

By default, no destination IP address or port number is configured for APs to report STA location data.

Format

private server { **ip-address** *ip-address* | **domain** *domain* } **port** *port-num* [**via-ac ac-port** *ac-port-num*]

undo private server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the server's IPv4 address to which APs report STA location data.	The value is in dotted decimal notation.
domain *domain*	Specifies the domain name to which APs report STA location data.	The value is a string of 1 to 255 characters.
port *port-num*	Specifies the destination port number on the location server to which APs directly report terminal location data. Specifies the destination port number on the location server to which APs report terminal location data through an AC.	The value is an integer that ranges from 1 to 65535.
via-ac	Indicates that STA location data is reported to the location server through an AC	-

Parameter	Description	Value
ac-port *ac-port-num*	Specifies the destination port number on the AC to which APs report STA location data.	The value is an integer that ranges from 5000 to 65535.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP completes channel scan, the AP can report the collected data to the location server in the following two methods.

- The AP directly reports the data to the location server.
- The AP reports the data to the location server through an AC.

When the AP and the location server are located on different LANs, the AP must report the data to the AC first. The AC must identify information about authorized and unauthorized STAs based on the location data and report the information to the location server.

If the route between the AP and location server is reachable, and the AC is not required to identify information about authorized and unauthorized STAs, configure the AP to send data to the location server directly, preventing adverse impact of the location function on AC performance and WLAN services.

Precautions

You cannot configure a port number that has been occupied by other services; otherwise, the port configuration fails.

For the same location method, via-ac can be configured only in one profile. If **via-ac** has been specified in the current location profile for a specific location method, it cannot be specified in other profiles for the same location method.

To set the protocol type to HTTP for APs to report information, specify **via-ac ac-port** *ac-port-num* in the command. If the UDP protocol is used and the domain name is specified, the parameter **via-ac ac-port** *ac-port-num* cannot be configured.

Example

Configure APs to report STA location data directly to the location server, and set the server's IP address and port number to **192.168.1.2** and **32180**, respectively.

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



```
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private server ip-address 192.168.1.2 port 32180
```

11.10.37 report enable

Function

The **report enable** command enables APs to send Bluetooth packets.

The **undo report enable** command disables APs from sending Bluetooth packets.

By default, an AP is disabled from sending Bluetooth packets.

Format

report enable

undo report enable

Parameters

None

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the Bluetooth tag location or Bluetooth data transparent transmission function is configured on an AP, run this command to enable the AP to send the Bluetooth packets to a location server or an AC.

Example

Enable APs to send Bluetooth packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] report enable
```

11.10.38 report-mode

Function

The **report-mode** command sets the mode and interval for APs to send Bluetooth packets.

The **undo report-mode** command cancels the configured mode and interval for APs to send Bluetooth packets.

By default, an AP sends Bluetooth packets at an interval of 10 seconds.

Format

report-mode { **immediate** | **periodic** [**interval** *interval*] }

undo report-mode

Parameters

Parameter	Description	Value
immediate	Enables APs to send Bluetooth packets immediately.	-
periodic	Enables APs to send Bluetooth packets periodically.	-
interval *interval*	Specifies an interval at which Bluetooth packets are sent.	The value is an integer that ranges from 1 to 600, in seconds.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP is enabled to report Bluetooth packet information, the AP reports Bluetooth packet information to the AC or location server. When APs are enabled to send Bluetooth packets immediately, the location accuracy is high but AP performance may be affected. When APs are enabled to send Bluetooth packets periodically, the location accuracy is low but AP performance is not affected.

Precautions

When APs are enabled to send Bluetooth packets periodically, set a proper interval at which Bluetooth packets are sent. Otherwise, location results may be inaccurate.

Example

Enable APs to send Bluetooth packets immediately.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] report-mode immediate
```

11.10.39 report-to-server

Function

The **report-to-server** command configures the destination server and port number to which APs report Bluetooth packets.

The **undo report-to-server** command restores the default destination server and port number to which APs report Bluetooth packets.

By default, no destination IP address or port number is configured for APs to report Bluetooth packets.

Format

report-to-server ip-address *ip-address* **port** *port-num* [**via-ac ac-port** *ac-port-num*]

report-to-server domain *domain* **port** *port-num*

undo report-to-server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IPv4 address of the location server to which APs report Bluetooth packets.	The value is in dotted decimal notation.
domain *domain*	Specifies the domain name of the location server to which APs report Bluetooth packets.	The value is a string of 1 to 255 characters.
port *port-num*	Specifies the destination UDP port number on the location server to which APs directly report Bluetooth packets. Specifies the destination UDP port number on the location server to which APs report Bluetooth packets through an AC.	The value is an integer that ranges from 1 to 65535.
via-ac	Specifies that Bluetooth packets are reported to a location server through an AC.	-

Parameter	Description	Value
ac-port *ac-port-num*	Specifies the destination UDP port number on the AC to which APs report Bluetooth packets.	The value is an integer that ranges from 5000 to 65535.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Bluetooth function is enabled, APs need to report collected Bluetooth data to a server. APs report the data using either of the following two methods:

- Reporting the data directly to the server
- Reporting the data to the server through an AC

Precautions

When configuring a port number, ensure that the port is not occupied by other services. If the port is occupied by other services, the port fails to be created.

For the same Bluetooth location function, Bluetooth data reporting through an AC can be configured only in one BLE profile. If Bluetooth data reporting through an AC has been configured in the current BLE profile for a Bluetooth location mode, the forwarding mode cannot be configured in other BLE profiles for the same Bluetooth location function.

Example

Enable APs to report Bluetooth packets to the server with destination IP address **192.168.1.2** and port number **8569**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] report-to-server ip-address 192.168.1.2 port 8569
```

11.10.40 reset wlan ble site-info

Function

The **reset wlan ble site-info** command deletes information about BLE devices stored on an AC.

Format

reset wlan ble site-info { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes information about all BLE devices.	-
mac-address *mac-address*	Deletes information about the BLE device with the specified MAC address from the device list on the AC.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the remaining aging time of BLE devices is long and some BLE devices are not in the current WLAN coverage area, but entries on the AC still exist, you can run this command to delete information about these BLE devices.

Precautions

Deleted information about BLE devices cannot be recovered. If the aging time of a BLE device is zero, information about the BLE device is automatically deleted from the device list on the AC.

Example

Delete information about all BLE devices from the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] reset wlan ble site-info all
```

11.10.41 reset wlan location device-info tag

Function

The **reset wlan location device-info tag** command clears tag information received by APs on the AC.

Format

reset wlan location device-info tag { **all** | **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
all	Clears tag information received by all APs.	-
ap-id *ap-id*	Clears tag information received by a specified AP ID.	The AP ID must exist.
ap-name *ap-name*	Clears tag information received by a specified AP name.	The AP name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

When tag information is too much, you can run this command to clear tag information received by APs on the AC. Cleared information cannot be recovered.

Example

Clear tag information received by all APs.

```
<HUAWEI> reset wlan location device-info tag all
```

11.10.42 sniffer enable

Function

The **sniffer enable** command enables and configures the working mode of an AP's built-in Bluetooth module.

The **undo sniffer enable** command disables the Bluetooth function of an AP's built-in Bluetooth module.

By default, the Bluetooth function of an AP's built-in Bluetooth module is disabled.

Format

sniffer enable { **ibeacon-mode** | **tag-mode** | **transparent-mode** }

undo sniffer enable

Parameters

Parameter	Description	Value
ibeacon-mode	Enables the Bluetooth monitoring function of an AP's built-in Bluetooth module.	-
tag-mode	Enables the Bluetooth tag location function of an AP's built-in Bluetooth module.	-
transparent-mode	Enables the Bluetooth data transparent transmission function of an AP's built-in Bluetooth module.	-

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Bluetooth monitoring or Bluetooth tag location function is enabled, the built-in Bluetooth module of an AP will scan and obtain information about surrounding BLE devices or Bluetooth tags. The built-in Bluetooth module then reports the obtained information such as MAC addresses, RSSIs, BLE broadcast frame contents, and battery power.

After the Bluetooth monitoring function is enabled, an AP obtains battery power information about surrounding BLE devices at WLAN service off-peak hours, for example, from 2:00 a.m. to 2:30 a.m. (system time), and then reports the obtained information to the AC. Precisely configure the system time of an AC to ensure that WLAN services are not affected when the AC obtains battery power of BLE devices.

After the Bluetooth data transparent transmission function is enabled, the built-in Bluetooth module of an AP scans surrounding Bluetooth clients, and reports information about the scanned Bluetooth clients, such as packet data, MAC addresses, and RSSIs. For BLE devices or Bluetooth terminals of some vendors, scan response frames can carry battery power information. The Bluetooth module also supports the query for battery level information. An AP periodically (at 2:00 am of the system time) sends scan request frames to surrounding BLE devices or Bluetooth terminals. After receiving the scan request frames, the BLE devices or Bluetooth terminals send scan response frames carrying battery power information. After receiving the scan response frames, the AP transparently transmits the frames to the AC or server.

The Bluetooth broadcast and Bluetooth monitoring functions can be enabled simultaneously for an AP's built-in Bluetooth module. When the two functions are both enabled, the AP's built-in Bluetooth module is also monitored.

After you run the **undo sniffer enable** command to disable the BLE monitoring or Bluetooth tag location function, the AC will trigger an alarm indicating that BLE devices or Bluetooth tags are offline.

Precautions

Enabling both the Bluetooth scanning and broadcast functions of an AP affects the efficiency for the AP's Bluetooth module to scan surrounding BLE devices. When an AP does not serve as a Bluetooth base station, it is recommended that the broadcast function of the AP be disabled.

Example

Enable the Bluetooth monitoring function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] sniffer enable ibeacon-mode
Warning: Modifying the monitoring mode may cause BLE devices in the original monitoring mode to go offline and age.
```

11.10.43 source (location profile view)

Function

The **source** command sets the source IP address used by the AC to send packets to a location server.

The **undo source** command deletes the configured source IP address.

By default, the source IP address used by the AC to send packets to a location server is not configured.

Format

source ip-address *ip-address*

undo source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the source IPv4 address used by the AC to send packets to a location server.	The value is in dotted decimal notation.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source IP address used by the AC to send packets to a location server is configured using the **source** command, the UDP packet sent from the AC to a location server carries this IP address as its source IP address.

Precautions

- Ensure that the AC IP address manually configured on a location server is the same as that configured using the **source** command.
- The source IP address must be a valid IP address existing on the device; otherwise, the configuration does not take effect.
- The source IP address in packets sent by an AC to a location server can be a global source IP address in the WLAN view and the source IP address in the location profile. The source IP address in the location profile takes precedence over the global source IP address in the WLAN view. If the source IP address in packets sent by an AC to a location server is not configured or the source IP address version is different from the IP address version of the location server, the AC's default IP address used for communicating with the location server is used as the source IP address.

Example

Configure the source IP address of the UDP packets sent from the AC to a location server as 10.102.25.23.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] source ip-address 10.102.25.23
```

11.10.44 source (BLE profile view)

Function

The **source** command sets the source IP address used by the AC to send packets to a location server.

The **undo source** command deletes the configured source IP address.

By default, the source IP address used by the AC to send packets to a location server is not configured, and the IP address of the route outbound interface is used as the source IP address.

Format

source ip-address *ip-address*

undo source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the source IPv4 address used by the AC to send packets to a location server.	The value is in dotted decimal notation.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Bluetooth location scenarios, after the source IP address used by the AC to send packets to a location server is configured using the **source** command, the packet sent from the AC to a location server carries this IP address as its source IP address.

Precautions

- Ensure that the AC IP address manually configured on a location server is the same as that configured using the **source** command.
- The source IP address must be a valid IP address existing on the device; otherwise, the configuration does not take effect.
- When the **source (BLE profile view)** and **ble source** commands are both executed, the function configured using the **source (BLE profile view)** command takes effect.

Example

Configure the source IP address of UDP packets sent from the AC to a location server as 10.102.25.23.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] source ip-address 10.102.25.23
```

11.10.45 tx-power (BLE profile view)

Function

The **tx-power** command configures the transmit power of an AP's built-in Bluetooth module.

The **undo tx-power** command restores the default transmit power of an AP's built-in Bluetooth module.

The default transmit power of an AP's built-in Bluetooth module is 0 dBm.

Format

tx-power *tx-power-value*

undo tx-power

Parameters

Parameter	Description	Value
tx-power-value	Specifies the transmit power of an AP's built-in Bluetooth module.	The value is of the enumerated type. The options are –21, –18, –15, –12, –9, –6, –3, 0, 1, 2, 3, 4, and 5, in dBm.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to change the transmit power of an AP's built-in Bluetooth module. Increasing the transmit power can improve Bluetooth signal transmission quality but causes more severe interference to other wireless devices. Reducing the transmit power can reduce interference to other wireless devices but affects Bluetooth signal transmission quality. Configure the transmit power of an AP's built-in Bluetooth module properly based on site requirements.

Precautions

After changing the transmit power of an AP's built-in Bluetooth module, you need to run the **broadcasting-content** command to reconfigure the RSSI calibration value in BLE broadcast frames.

Example

Set the transmit power of an AP's built-in Bluetooth module to 2 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] tx-power 2
```


11.11 WLAN Security Configuration Commands

11.11.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.11.2 anti-attack flood blacklist enable

Function

The **anti-attack flood blacklist enable** command enables the flood blacklist function.

The **undo anti-attack flood blacklist enable** command disables the flood blacklist function.

By default, the flood blacklist function is disabled.

Format

anti-attack flood { **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **blacklist enable**

undo anti-attack flood { **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **blacklist enable**

Parameters

Parameter	Description	Value
arp	Indicates whether to enable the ARP flood blacklist function.	-
dhcp	Indicates whether to enable the DHCP flood blacklist function.	-
dhcpv6	Indicates whether to enable the DHCPv6 flood blacklist function.	-
igmp	Indicates whether to enable the IGMP flood blacklist function.	-
mdns	Indicates whether to enable the mDNS flood blacklist function.	-

Parameter	Description	Value
nd	Indicates whether to enable the ND flood blacklist function.	-
other-broadcast	Indicates whether to enable the flood blacklist function for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Indicates whether to enable the flood blacklist function for multicast packets other than IGMP and mDNS packets.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the protocol-based flood blacklist function is enabled, the device considers traffic of a specified protocol (such as DHCP or ARP) with a rate higher than that specified in **anti-attack flood sta-rate-threshold** a flood attack and adds the STA to the blacklist.

Prerequisites

The flood prevention function has been enabled using the **undo anti-attack flood disable** command.

Example

Enable the DHCP flood blacklist function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name profile1
[HUAWEI-wlan-vap-prof-profile1] anti-attack flood dhcp blacklist enable
```

11.11.3 anti-attack flood disable

Function

The **anti-attack flood disable** disables the flood prevention function.

The **undo anti-attack flood disable** command enables the flood prevention function.

By default, the flood prevention function is enabled.

Format

anti-attack flood { **all** | **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **disable**

undo anti-attack flood { **all** | **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **disable**

Parameters

Parameter	Description	Value
all	Indicates whether to enable the flood prevention function for ARP, DHCP, DHCPv6, IGMP, mDNS, and ND multicast, broadcast, and unicast packets.	-
arp	Indicates whether to enable the ARP flood prevention function.	-
dhcp	Indicates whether to enable the DHCP flood prevention function.	-
dhcpv6	Indicates whether to enable the DHCPv6 flood prevention function.	-
igmp	Indicates whether to enable the IGMP flood prevention function.	-
mdns	Indicates whether to enable the mDNS flood prevention function.	-
nd	Indicates whether to enable the ND flood prevention function.	-

Parameter	Description	Value
other-broadcast	Indicates whether to enable the flood prevention function for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Indicates whether to enable the flood prevention function for multicast packets other than IGMP and mDNS packets.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a large number of packets are sent to a device in a short time, the device becomes busy processing the packets and cannot process normal services. To prevent flood attacks, you can configure protocol-based flood prevention.

Precautions

The flood prevention function takes effect only for incoming traffic on an AP's wired interface.

Example

Disable the DHCP flood prevention function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name profile1
[HUAWEI-vap-prof-profile1] anti-attack flood dhcp disable
```

11.11.4 anti-attack flood sta-rate-threshold

Function

The **anti-attack flood sta-rate-threshold** command sets the flood threshold.

The **undo anti-attack flood sta-rate-threshold** command restores the default flood threshold.

The default flood threshold is 4 pps for ARP, DHCP, DHCPv6, IGMP, and mDNS packets, 8 pps for ND packets, 10 pps for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets, and 10 pps for multicast packets other than IGMP and mDNS packets.

Format

anti-attack flood { **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **sta-rate-threshold** *sta-rate-threshold*

undo anti-attack flood { **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **sta-rate-threshold**

Parameters

Parameter	Description	Value
arp	Specifies ARP packets.	-
dhcp	Specifies DHCP packets.	-
dhcpv6	Specifies DHCPv6 packets.	-
igmp	Specifies IGMP packets.	-
mdns	Specifies mDNS packets.	-
nd	Specifies ND packets.	-
other-broadcast	Specifies broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Specifies multicast packets other than IGMP and mDNS packets.	-
sta-rate-threshold	Specifies the rate threshold of broadcast traffic from STAs.	For **arp**, **dhcp**, **dhcpv6**, and **nd**, the value is an integer that ranges from 1 to 5000, in pps. For **igmp**, **mdns**, **other-broadcast**, and **other-multicast**, the value is an integer that ranges from 0 to 5000, in pps.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the flood prevention function is enabled, you can run this command to set the broadcast traffic threshold.

When the traffic rate exceeds the threshold, the device considers a flood attack from the STA and discards the traffic. This prevents the upper-layer network from being affected by the flood.

If the flood blacklist function is enabled using the **anti-attack flood blacklist enable** command, the device adds flood STAs to the blacklist.

Prerequisites

The flood prevention function has been enabled using the **undo anti-attack flood disable** command.

Precautions

The flood prevention function takes effect only for incoming traffic on an AP's wired interface.

Example

Set the DHCP flood threshold to 100 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name profile1
[HUAWEI-vap-prof-profile1] anti-attack flood dhcp sta-rate-threshold 100
```

11.11.5 arp anti-attack check user-bind enable

Function

The **arp anti-attack check user-bind enable** command enables dynamic ARP inspection (DAI).

The **undo arp anti-attack check user-bind enable** command disables DAI.

By default, DAI is disabled.

Format

arp anti-attack check user-bind enable

undo arp anti-attack check user-bind enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

DAI allows an AP to detect the ARP Request and Reply packets transmitted on the VAPs of the AP, to discard invalid and attack ARP packets, and to send an alarm to the connected AC. This function prevents ARP packets of unauthorized users from accessing the external network through the AP, protecting authorized users against interference or spoofing, and protecting the AP.

- Invalid ARP packets: The source IP and MAC addresses of ARP Request and Reply packets do not match.
- Attack ARP packets: When an AP receives a large number of consecutive ARP packets and the number of ARP packets exceeds the ARP attack alarm threshold, an ARP attack occurs.

Example

Enable DAI.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] arp anti-attack check user-bind enable
```

11.11.6 attack-device trap enable

Function

The **attack-device trap enable** command enables the alarm function for attack detection.

The **undo attack-device trap enable** command disables the alarm function for attack detection.

By default, the alarm function for attack detection is disabled.

Format

attack-device trap enable

undo attack-device trap enable

Parameters

None

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is executed, an alarm is triggered immediately when the device detects an attack.

Prerequisites

The attack detection function has been enabled by using the **wids attack detect** command.

Precautions

If a large number of attack devices exist, enabling this function will trigger a large number of alarms and generate a large number of logs. Therefore, you are advised to use this function together with a log server.

Example

Enable the alarm function for attack detection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] attack-device trap enable
```

11.11.7 brute-force-detect interval

Function

The **brute-force-detect interval** command sets the interval for brute force key cracking detection.

The **undo brute-force-detect interval** command restores the default interval for brute force key cracking detection.

By default, the interval for brute force key cracking detection is 60 seconds.

Format

brute-force-detect interval *interval*

undo brute-force-detect interval

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for brute force key cracking detection.	The value is an integer that ranges from 10 to 120, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a brute force key cracking attack, an attacker tries all possible key combinations one by one to obtain the correct password. To improve password security, enable defense against brute force key cracking to prolong the time used to crack passwords.

An AP checks whether the number of key negotiation failures during WPA/WPA2-PSK, WAPI-PSK, or WEP-Share-Key authentication of a user exceeds the threshold configured using the **brute-force-detect threshold** command. If so, the AP considers that the user is using the brute force method to crack the password and reports an alarm to the AC. If the dynamic blacklist function is enabled, the AP adds the user to the dynamic blacklist and discards all the packets from the user until the dynamic blacklist entry ages out.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the interval for brute force key cracking detection to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect wpa-psk enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] brute-force-detect interval 100
```


11.11.8 brute-force-detect quiet-time

Function

The **brute-force-detect quiet-time** command sets the quiet time for an AP to report brute force key attacks to an AC.

The **undo brute-force-detect quiet-time** command restores the default quiet time for an AP to report brute force key attacks to an AC.

By default, the quiet time for an AP to report brute force key attacks to an AC is 600 seconds.

Format

brute-force-detect quiet-time *quiet-time-value*

undo brute-force-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report brute force key attacks to an AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repeated alarms are generated. To prevent this situation, configure the quiet time function for attack detection. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the quiet time for an AP to report brute force key attacks to an AC to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect wpa-psk enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] brute-force-detect quiet-time 300
```

11.11.9 brute-force-detect threshold

Function

The **brute-force-detect threshold** command sets the maximum number of key negotiation failures allowed within a brute force key cracking attack detection period.

The **undo brute-force-detect threshold** command restores the default maximum number of key negotiation failures allowed within a brute force key cracking attack detection period.

By default, an AP allows a maximum of 20 key negotiation failures within a brute force key cracking attack detection period.

Format

brute-force-detect threshold *threshold*

undo brute-force-detect threshold

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the number of key negotiation failures within a detection period.	The value is an integer that ranges from 1 to 100.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a brute force key cracking attack, an attacker tries all possible key combinations one by one to obtain the correct password. To improve password security, enable defense against brute force key cracking to prolong the time used to crack passwords.

An AP checks whether the number of key negotiation failures during WPA/WPA2-PSK, WAPI-PSK, or WEP-Share-Key authentication of a user exceeds the threshold configured using the **brute-force-detect threshold** command. If so, the AP considers that the user is using the brute force method to crack the password and reports an alarm to the AC. If the dynamic blacklist function is enabled, the AP adds the user to the dynamic blacklist and discards all the packets from the user until the dynamic blacklist entry ages out. If the threshold is set to a small value, the AP may incorrectly add authorized users to the dynamic blacklist, causing the users unable to go online.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the maximum number of key negotiation failures allowed within a brute force key cracking attack detection period to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect wpa-psk enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] brute-force-detect threshold 60
```

11.11.10 contain

Function

The **contain** command enables containment of rogue and interfering devices based on the RSSI and number of associated STAs on the devices.

The **undo contain** command disables containment of rogue and interfering devices based on the RSSI and number of associated STAs on the devices.

By default, containment of rogue and interfering devices based on the RSSI and number of associated STAs on the devices is disabled.

Format

contain { **min-rssi** *min-rssi* | **min-sta-num** *min-sta-num* }

undo contain { **min-rssi** | **min-sta-num** }

Parameters

Parameter	Description	Value
min-rssi *min-rssi*	Specifies the minimum RSSI value.	The value is an integer that ranges from -95 to -50.
min-sta-num *min-sta-num*	Specifies the minimum number of associated STAs.	The value is an integer that ranges from 1 to 10.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After RSSI-based containment is enabled, if the RSSIs of detected rogue and interfering devices are no more than the specified minimum RSSI value, the devices are not contained. They are contained only when their RSSIs exceed the specified minimum RSSI value.

After containment based on the number of associated STAs is enabled, if the number of STAs associated with detected rogue and interfering devices is smaller than the specified minimum value, the devices are not contained. They are contained only when the number of STAs associated with them reaches the specified minimum value.

Prerequisites

Detection and containment of rogue and interfering devices have been enabled.

Precautions

This function is not supported in manual containment mode.

Example

Enable containment of rogue and interfering APs with spoofing SSIDs and set the number of associated STAs that triggers containment to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids contain enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
```



```
[HUAWEI-wlan-wids-prof-default] contain-mode spoof-ssid-ap
[HUAWEI-wlan-wids-prof-default] contain min-sta-num 5
```

11.11.11 contain-mode

Function

The **contain-mode** command sets the containment mode against rogue or interference devices.

The **undo contain-mode** command deletes the containment mode against rogue or interference devices.

By default, no containment mode against rogue or interference devices is set.

Format

contain-mode { **open-ap** | **spoof-ssid-ap** | **client** [**protect sta-whitelist-profile** *profile-name*] | **adhoc** }

undo contain-mode { **open-ap** | **spoof-ssid-ap** | **client** [**protect**] | **adhoc** }

Parameters

Parameter	Description	Value
open-ap	Sets the containment mode against open-authentication rogue or interference APs.	-
spoof-ssid-ap	Sets the containment mode against rogue or interference APs using spoofing SSIDs.	-
client	Sets the containment mode against unauthorized STAs or interference STAs.	-
protect sta-whitelist-profile *profile-name*	Protects STAs based on the STA whitelist. Authorized STAs in the whitelist are protected from connecting to rogue or interference APs.	-
adhoc	Sets the containment mode against Ad-hoc devices.	-

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Rogue or interference devices pose serious security threats to enterprise networks.

After the containment mode is set against rogue or interference APs, the monitor AP uses the identity of the rogue or interference AP to broadcast deauthentication frames to forcibly disconnect STAs. To prevent the STAs from connecting to the rogue or interference AP again, the monitor AP will periodically and continuously send deauthentication frames.

After the containment mode is set against rogue STAs, interference STAs or Ad-hoc devices, the monitor AP uses the MAC address of a rogue device to continuously send unicast deauthentication frames.

Example

Counter rogue and interference APs with spoofing SSIDs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids contain enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] contain-mode spoof-ssid-ap
```

11.11.12 device report-interval

Function

The **device report-interval** command sets the interval at which an AP reports incremental wireless device information.

The **undo device report-interval** command restores the default interval at which an AP reports incremental wireless device information.

By default, an AP reports incremental wireless device information to an AC at an interval of 300 seconds.

Format

device report-interval *interval*

undo device report-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an AP reports incremental wireless device information.	The value is an integer that ranges from 60 to 3600, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The monitoring AP buffers information about detected wireless devices at the interval set using the **device report-interval** command. When the interval is reached, the monitoring AP reports the information to the AC and then clears the reported information.

Prerequisites

The device detection function has been enabled using the **wids device detect enable** command for the AP.

Example

Set the interval at which an AP reports incremental wireless device information to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids device detect enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] device report-interval 120
```

11.11.13 dhcp trust port

Function

The **dhcp trust port** command configures a DHCP trusted interface on an AP.

The **undo dhcp trust port** command cancels the configuration.

By default, the DHCP trusted interface is enabled on the AP's uplink interface in the AP wired port profile view.

Format

dhcp trust port

undo dhcp trust port

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before WLAN services are delivered to an AP, run the **dhcp trust port** command in the AP wired port profile view. After the command is run, the AP receives the DHCP OFFER, ACK, and NAK packets sent by the authorized DHCP server and forwards the packets to STAs so that the STAs can obtain valid IP addresses and go online.

The **undo dhcp trust port** command configured in the AP wired port profile view takes effect only in direct forwarding mode, but not in tunnel forwarding mode.

Precautions

When executed in the AP wired port view, this command takes effect only on uplink interfaces of an AP. To configure a downlink wired interface on an AP as a DHCP trusted interface, you only need to run the **learn-client-address enable (AP wired port profile view)** command to enable STA address learning, but do not need to run the **dhcp trust port** command.

Example

Create an AP wired port profile named **wire1**, and enable a DHCP trusted interface on an AP in this profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] dhcp trust port
```

11.11.14 display ap radio-environment

Function

The **display ap radio-environment** command displays air interface environment information about AP radios.

Format

display ap radio-environment { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays air interface environment information about radios of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays air interface environment information about radios of the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Displays air interface environment information about the AP radio with a specified ID.	The radio ID must exist.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When WLAN access experience is poor, you can run this command to view air interface environment information and Wi-Fi interference sources. The interference can be determined based on the noise floor, signal to interference plus noise ratio (SINR), co-channel interference, and adjacent-channel interference. After this command is executed, radio scanning of the AP is automatically enabled, and the AP starts to scan the air interface environment of radios. You can run this command again to view air interface environment scanning results.

Precautions

When you run this command for the first time, no air interface environment scanning result is displayed. To view air interface environment scanning results, run this command again.

After AP radio scanning is enabled using this command, the air interface performance of an AP is affected. If this command is not executed again after five minutes, AP radio scanning is automatically disabled.

If the **radio** *radio-id* parameter is not specified, air interface environment information about all radios of the AP is displayed.

NOTE

In the scanning result, the channel utilization, co-channel interference, and adjacent-channel interference are calculated with the impact of non-Wi-Fi interference. However, non-Wi-Fi interference devices are not displayed in the interference source list.

Example

Display air interface environment information about radio 0 of AP 1.

```
<HUAWEI> display ap radio-environment ap-id 1 radio 0
Warning: This operation will enable scanning for the specified radio, affecting AP's air interface
performance. Scanning will be automatically disabled 5 minutes after this command is run. Continue? [Y/
N]y
Info: This operation may take a few seconds. Please wait for a moment.done.
p:            permit
i:           interference
Ch:           Channel
CU:           Channel Utility
NF:           Noise Floor
CommIf:       Common-Channel Interference
AdjaceIf:     Adjacent-Channel Interference
SINR:         Signal to Interference and Noise Ratio
#Neighbors:   Number of Neighbors detected
Radio:        0
ScanChannel:  1
WorkChannel:  1
ScanCycle:    1
--------------------------------------------------------------------------------
Ch  NF   CU(%) CommIf(%) AdjaceIf(%) SINR      #Neighbors
--------------------------------------------------------------------------------
1   -105 75    19        -           245       57
--------------------------------------------------------------------------------
Total: 1
--------------------------------------------------------------------------------
Ch    MAC            Type  RSSI  SSID
--------------------------------------------------------------------------------
1     00e0-fc3a-8d41 i     -65   xw9-2g-tunnel
------------------------------------------------
Total: 1
```

Table 11-208 Description of the **display ap radio-environment** { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] command output

Item	Description
Radio	Radio on which the air interface environment is scanned.
ScanChannel	Scanning channel.
WorkChannel	Working channel of the AP.
ScanCycle	Scanning count.
Ch	Channel that has scanned a device.
NF	Noise floor.
CU(%)	Channel utilization.
CommIf(%)	Co-channel interference.
AdjaceIf(%)	Adjacent-channel interference.
#Neighbors	Number of scanned radio neighbors.
SINR	Signal to interference plus noise ratio (SINR).

Item	Description
MAC	MAC address of the scanned device.
Type	Type of the scanned interference device. • i: WIDS device • p: Non-WIDS device
RSSI	RSSI of the scanned device.
SSID	SSID to which the scanned device is connected.

NOTE

If an AP detects that a channel has a high co-channel interference (higher than 50%), another Wi-Fi device is using this channel and affects the local AP. In this case, it is recommended that the AP channel be switched using radio calibration or other methods.

11.11.15 display references wids-whitelist-profile

Function

The **display references wids-whitelist-profile** command displays reference information about a WIDS whitelist profile.

Format

display references wids-whitelist-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WIDS whitelist profile.	The WIDS whitelist profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wids-whitelist-profile** command to view reference information about a WIDS whitelist profile.

Example

Display reference information about the WIDS whitelist profile **default**.

```
<HUAWEI> display references wids-whitelist-profile name default
------------------------------------------------------------
Profile type                Reference name
------------------------------------------------------------
wids-profile                default
------------------------------------------------------------
Total: 1
```

Table 11-209 Description of the **display references wids-whitelist-profile** command output

Item	Description
Profile type	Type of the profile that references the WIDS whitelist profile.
Reference name	Name of the profile that references the WIDS whitelist profile.

11.11.16 display references wids-profile

Function

The **display references wids-profile** command displays reference information about a WIDS profile.

Format

display references wids-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WIDS profile.	The WIDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wids-profile** command to view reference information about a WIDS profile.

Example

Display reference information about the WIDS profile **default**.

```
<HUAWEI> display references wids-profile name default
------------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------------
AP group                    default
------------------------------------------------------------------------------
Total: 1
```

Table 11-210 Description of the **display references wids-profile** command output

Item	Description
Reference type	Type of the object that references the WIDS profile.
Reference name	Name of the object that references the WIDS profile.

11.11.17 display references wids-spoof-profile

Function

The **display references wids-spoof-profile** command displays reference information about a WIDS spoof SSID profile.

Format

display references wids-spoof-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WIDS spoof SSID profile.	The WIDS spoof SSID profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wids-spoof-profile** command to view reference information about a WIDS spoof SSID profile.

Example

Display reference information about the WIDS spoof SSID profile **default**.

```
<HUAWEI> display references wids-spoof-profile name default
Profile type                  Reference name
--------------------------------------------------------------
wids-profile                  default
--------------------------------------------------------------
Total: 1
```

Table 11-211 Description of the **display references wids-spoof-profile** command output

Item	Description
Profile type	Type of the profile that references the WIDS spoof SSID profile.
Reference name	Name of the profile that references the WIDS spoof SSID profile.

11.11.18 display wids-whitelist-profile

Function

The **display wids-whitelist-profile** command displays information about a WIDS whitelist profile.

Format

display wids-whitelist-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WIDS whitelist profiles.	-
name *profile-name*	Displays information about a specified WIDS whitelist profile.	The WIDS whitelist profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wids-whitelist-profile** command to view information about a WIDS whitelist profile.

Example

Display information about all WIDS whitelist profiles.

```
<HUAWEI> display wids-whitelist-profile all
------------------------------------------------------------
Profile name                Reference
------------------------------------------------------------
default                      1
------------------------------------------------------------
Total: 1
```

Table 11-212 Description of the **display wids-whitelist-profile all** command output

Item	Description
Profile name	Specifies the name of a WIDS whitelist profile.
Reference	Number of times a WIDS whitelist profile is referenced.

Display information about the WIDS whitelist profile **default**.

```
<HUAWEI> display wids-whitelist-profile name default
------------------------------------------------------------
Permit AP OUI SSID match : both
------------------------------------------------------------
Type        Content
```



```
------------------------------------------------------------
MAC          00e0-fc12-3456
OUI          00-e0-fc
SSID         example
------------------------------------------------------------
Total: 3
```

Table 11-213 Description of the **display wids-whitelist-profile name** command output

Item	Description
Permit AP OUI SSID match	Rules for matching OUIs and SSIDs in the WIDS whitelist: • both: Both OUIs and SSIDs can be matched. • any: Either of OUIs and SSIDs can be matched. The default value is **both**. To set the rule, run the **permit-ap oui-ssid-match** command.
Type	Type of authorized APs.
Content	Rule for authorized APs. To set the rule, run the **permit-ap** command.

11.11.19 display wids-profile

Function

The **display wids-profile** command displays information about a WIDS profile.

Format

display wids-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WIDS profiles.	-
name *profile-name*	Displays information about a specified WIDS profile.	The WIDS profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wids-profile** command to view information about a WIDS profile.

Example

Display information about all WIDS profiles.

```
<HUAWEI> display wids-profile all
------------------------------------------------------------
Profile name                Reference
------------------------------------------------------------
default                      1
------------------------------------------------------------
Total: 1
```

Table 11-214 Description of the **display wids-profile all** command output

Item	Description
Profile name	Name of a WIDS profile.
Reference	Number of times a WIDS profile is referenced.

Display information about the WIDS profile **default**.

```
<HUAWEI> display wids-profile name default
------------------------------------------------------------
Device report interval(s)          : 60
Brute force detect interval(s)     : 20
Brute force detect threshold       : 20
Brute force quiet time(s)          : 600
Flood detect interval(s)           : 10
Flood detect threshold             : 1
Flood quiet time(s)                : 600
Weak IV quiet time(s)              : 600
Spoof quiet time(s)                : 600
Dynamic blacklist                  : enable
Contain rogue mode                 : spoof SSID AP
                                     open-authentication rogue AP
                                     client
                                     client protect
                                     Ad hoc
Contain minimum RSSI(dBm)          : -
Contain minimum sta number         : -
Attack device trap switch          : disable
STA whitelist profile              : STA_whitelist
WIDS spoof profile                 : default
WIDS whitelist profile             : default
------------------------------------------------------------
```


Table 11-215 Description of the **display wids-profile name** command output

Item	Description
Device report interval(s)	Interval at which an AP reports the detected incremental wireless device information. To configure this parameter, run the **device report-interval** command.
Brute force detect interval(s)	Interval for brute force key cracking detection. To configure this parameter, run the **brute-force-detect interval** command.
Brute force detect threshold	Maximum number of key negotiation failures allowed within a brute force key cracking detection period. To configure this parameter, run the **brute-force-detect threshold** command.
Brute force quiet time(s)	Quiet time for an AP to report the detected brute force attacks to the AC. To configure this parameter, run the **brute-force-detect quiet-time** command.
Flood detect interval(s)	Flood attack detection interval. To configure this parameter, run the **flood-detect interval** command.
Flood detect threshold	Flood attack detection threshold. To configure this parameter, run the **flood-detect threshold** command.
Flood quiet time(s)	Quiet time for an AP to report the detected flood attacks to the AC. To configure this parameter, run the **flood-detect quiet-time** command.
Weak IV quiet time(s)	Quiet time for an AP to report the detected weak IV attacks to the AC. To configure this parameter, run the **weak-iv-detect quiet-time** command.
Spoof quiet time(s)	Quiet time for an AP to report the detected spoofing attacks to the AC. To configure this parameter, run the **spoof-detect quiet-time** command.

Item	Description
Dynamic blacklist	Whether the dynamic blacklist function is enabled. To configure this parameter, run the **dynamic-blacklist disable** command.
Contain rogue mode	Containment mode against rogue devices. To configure this parameter, run the **contain-mode** command.
Contain minimum RSSI(dBm)	Minimum RSSI value for containing rogue and interfering devices based on the RSSI of the devices. To configure this parameter, run the **contain** command.
Contain minimum sta number	Minimum number of associated STAs for containing rogue and interfering devices based on the number of STAs associated with the devices. To configure this parameter, run the **contain** command.
Attack device trap switch	Whether the alarm function for attack detection is enabled. To configure this parameter, run the **attack-device trap enable** command.
STA whitelist profile	STA protection based on a STA whitelist. To configure this parameter, run the **contain-mode** command.
WIDS spoof profile	WIDS spoof SSID profile bound to the WIDS profile. To configure this parameter, run the **wids-spoof-profile (WIDS profile view)** command.
WIDS whitelist profile	WIDS whitelist profile bound to the WIDS profile. To configure this parameter, run the **wids-whitelist-profile (WIDS profile view)** command.

11.11.20 display wids-spoof-profile

Function

The **display wids-spoof-profile** command displays information about a WIDS spoof SSID profile.

Format

display wids-spoof-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WIDS spoof SSID profiles.	-
name *profile-name*	Displays information about a specified WIDS spoof SSID profile.	The WIDS spoof SSID profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wids-spoof-profile** command to view information about a WIDS spoof SSID profile.

Example

Display information about all WIDS spoof SSID profiles.

```
<HUAWEI> display wids-spoof-profile all
------------------------------------------------------------
Profile name                Reference
------------------------------------------------------------
default                      1
------------------------------------------------------------
Total: 1
```

Table 11-216 Description of the **display wids-spoof-profile all** command output

Item	Description
Profile name	Name of a WIDS spoof SSID profile.

Item	Description
Reference	Number of times a WIDS spoof SSID profile is referenced.

Display information about the WIDS spoof SSID profile **default**.

```
<HUAWEI> display wids-spoof-profile name default
-------------------------------------------------------------
ID      Pattern rule
-------------------------------------------------------------
0       ^HUAWE[1l]$
-------------------------------------------------------------
Total: 1
```

Table 11-217 Description of the **display wids-spoof-profile name** command output

Item	Description
ID	Index.
Pattern rule	Matching rule for spoofing SSIDs. To set the matching rule, run the **spoof-ssid** command.

11.11.21 display references security-profile

Function

The **display references security-profile** command displays reference information about a security profile.

Format

display references security-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified security profile.	The security profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a security profile.

Example

Display reference information about the security profile **security-profile1**.

```
<HUAWEI> display references security-profile name security-profile1
-----------------------------------------------
Reference type          Reference name
-----------------------------------------------
VAP profile             vap-profile1
-----------------------------------------------
Total: 1
```

Table 11-218 Description of the **display references security-profile** command output

Item	Description
Reference type	Type of the profile that references a security profile.
Reference name	Name of the profile that references a security profile.

11.11.22 display references sta-blacklist-profile

Function

The **display references sta-blacklist-profile** command displays reference information about a STA blacklist profile.

Format

display references sta-blacklist-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a STA blacklist profile.	The STA blacklist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a STA blacklist profile.

Example

Display reference information about the STA blacklist profile **sta-blacklist-profile1**.

```
<HUAWEI> display references sta-blacklist-profile name sta-blacklist-profile1
-----------------------------------------------
Reference type          Reference name
-----------------------------------------------
VAP profile             vap-profile1
-----------------------------------------------
Total: 1
```

Table 11-219 Description of the **display references sta-blacklist-profile** command output

Item	Description
Reference type	Type of the profile that references the STA blacklist profile.
Reference name	Name of the profile that references the STA blacklist profile.

11.11.23 display references sta-whitelist-profile

Function

The **display references sta-whitelist-profile** command displays reference information about a STA whitelist profile.

Format

display references sta-whitelist-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a STA whitelist profile.	The STA whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a STA whitelist profile.

Example

Display reference information about the STA whitelist profile **sta-whitelist-profile1**.

```
<HUAWEI> display references sta-whitelist-profile name sta-whitelist-profile1
-----------------------------------------------
Reference type          Reference name
-----------------------------------------------
VAP profile             vap-profile1
-----------------------------------------------
Total: 1
```

Table 11-220 Description of the **display references sta-whitelist-profile** command output

Item	Description
Reference type	Type of the profile that references the STA whitelist profile.
Reference name	Name of the profile that references the STA whitelist profile.

11.11.24 display security-profile

Function

The **display security-profile** command displays configuration and reference information about a security profile.

Format

display security-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all security profiles.	-
name *profile-name*	Displays information about a specified security profile.	The security profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view configuration and reference information about a specified security profile or all security profiles.

Example

Display information about all security profiles.

```
<HUAWEI> display security-profile all
-------------------------------------------------------------
Profile name                Reference
-------------------------------------------------------------
default                     1
default-wds                 1
default-mesh                1
security-profile1           0
-------------------------------------------------------------
Total: 4
```

Table 11-221 Description of the **display security-profile all** command output

Item	Description
Profile name	Name of the security profile.
Reference	Number of times a security profile is referenced.

Display information about the security profile **default**.

```
<HUAWEI> display security-profile name default
-------------------------------------------------------------
Security policy             : Open system
Encryption                  : -
-------------------------------------------------------------
WEP's configuration
```



```
Key 0                       : *****
Key 1                       : *****
Key 2                       : *****
Key 3                       : *****
Default key ID              : 0
------------------------------------------------------------
WPA/WPA2's configuration
PTK update                  : disable
PTK update interval(s)      : 43200
------------------------------------------------------------
WAPI's configuration
CA certificate filename     : -
ASU certificate filename    : -
AC certificate filename     : -
AC private key filename     : -
AC local key pair name      : -
WAPI source interface       : -
Authentication server IP    : -
WAI timeout(s)              : 60
BK update interval(s)       : 43200
BK lifetime threshold(%)    : 70
USK update method           : Time-based
USK update interval(s)      : 86400
MSK update method           : Time-based
MSK update interval(s)      : 86400
Cert auth retrans count     : 3
USK negotiate retrans count : 3
MSK negotiate retrans count : 3
------------------------------------------------------------
```


Table 11-222 Description of the **display security-profile name** command output

Item	Description
Security policy	Security policy. The following security policies are supported: ● Open system: WEP open system authentication ● Share key: WEP shared key authentication ● WEP 802.1x: Dynamic WEP ● WPA 802.1x: WPA-802.1X ● WPA2 802.1x: WPA2-802.1X ● WPA-WPA2 802.1x: WPA-WPA2-802.1X ● WPA PSK ● WPA2 PSK ● WPA-WPA2 PSK ● WPA PPSK ● WPA2 PPSK ● WPA-WPA2 PPSK ● WPA3 SAE ● WPA3 802.1x: WPA3-802.1X ● WPA2-WPA3 PSK-SAE ● WPA2-WPA3 802.1x: WPA2-WPA3-802.1X ● WAPI PSK ● WAPI certificate ● OWE ● WPA2 RPSK ● -: No security policy To configure this parameter, run the **security wep**, **security dot1x**, **security psk**, **security wpa2-wpa3 psk-sae**, **security wpa3 sae**, **security wpa3 dot1x**, **security enhanced-open aes**, or **security wapi** command.

Item	Description
Encryption	Encryption mode. The following encryption modes are supported: GCMP-256, TKIP, AES, AES-TKIP, WEP-40, WEP-104, WEP-128, and SMS4. The WAPI encryption mode is fixed to SMS4, the hybrid WPA3-SAE +WPA2-WPA3 encryption mode is fixed to AES, and the WPA3-802.1X encryption mode is fixed to GCMP-256 + AES, and the OWE encryption mode is fixed to AES. To configure this parameter, run the **wep key**, **security dot1x**, **security wpa2-wpa3 psk-sae**, **security wpa3 sae**, **security wpa3 dot1x**, **security enhanced-open aes**, **security wpa2-wpa3 dot1x**, or **security psk** command.
PMF	Whether the Protected Management Frame (PMF) function of a VAP is enabled. ● **disable**: This function is disabled. ● **optional**: This function is enabled in optional mode. ● **mandatory**: This function is forcibly enabled. This line is displayed in the command output only when the authentication and encryption mode is WPA2-AES/ WPA3/OWE. To configure this parameter when the authentication mode is WPA2-AES, run the **pmf** command. When the authentication mode is WPA3, this parameter is unconfigurable. The value of this parameter is fixed at **mandatory** when the authentication mode is WPA3-SAE or WPA3-802.1X and **optional** when the authentication mode is WPA2-WPA3. When the authentication mode is OWE or its transition mode, the value of this parameter is fixed at **mandatory**.
Key *key-id*	Key ID. To configure this parameter, run the **wep key** command.

Item	Description
Default key ID	Default key ID. To configure this parameter, run the **wep default-key** command.
PTK update	Whether to enable periodic PTK update in WPA, WPA2, or WPA-WPA2 authentication and encryption. ● enable: This function is enabled. ● disable: This function is disabled. To configure this parameter, run the **wpa ptk-update enable** command.
PTK update interval(s)	The interval for updating PTKs in WPA, WPA2, or WPA-WPA2 authentication and encryption. The value is an integer in seconds. To configure this parameter, run the **wpa ptk-update ptk-update-interval** command.
CA certificate filename	CA certificate file name. To configure this parameter, run the **wapi import certificate** command.
ASU certificate filename	File name of the authentication server unit (ASU) certificate. To configure this parameter, run the **wapi import certificate** command.
AC certificate filename	AC certificate file name. To configure this parameter, run the **wapi import certificate** command.
AC private key filename	AC private key file name. To configure this parameter, run the **wapi import private-key** command.
AC local key pair name	Name of the local ECC key pair on the AC. To configure this parameter, run the **wapi import private-key** command.
WAPI source interface	WAPI source interface. To configure this parameter, run the **wapi source interface** command.
Authentication server IP	IP address of the ASU certificate server. To configure this parameter, run the **wapi asu** command.

Item	Description
WAI timeout(s)	Timeout period of an association. To configure this parameter, run the **wapi sa-timeout** command.
BK update interval(s)	Interval for updating the base key (BK). To configure this parameter, run the **wapi bk** command.
BK lifetime threshold(%)	Threshold for triggering BK update. To configure this parameter, run the **wapi bk** command.
USK update method	Whether the USK is updated based on a time interval or a packet count. To configure this parameter, run the **wapi key-update** command.
USK update interval(s)	Interval for updating the unicast session key (USK). To configure this parameter, run the **wapi usk** command.
MSK update method	Whether the MSK is updated based on a time interval or a packet count. To configure this parameter, run the **wapi key-update** command.
MSK update interval(s)	Interval for updating the MBMS service key (MSK). To configure this parameter, run the **wapi msk** command.
Cert auth retrans count	Number of retransmissions of certificate authentication packets. To configure this parameter, run the **wapi cert-retrans-count** command.
USK negotiate retrans count	Number of retransmissions of USK negotiation packets. To configure this parameter, run the **wapi usk** command.
MSK negotiate retrans count	Number of retransmissions of MSK negotiation packets. To configure this parameter, run the **wapi msk** command.

11.11.25 display sta-blacklist-profile

Function

The **display sta-blacklist-profile** command displays configuration and reference information about a STA blacklist profile.

Format

display sta-blacklist-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all STA blacklist profiles.	-
name *profile-name*	Displays information about a specified STA blacklist profile.	The STA blacklist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring STA blacklists on a device, you can run this command to check whether a MAC address is in the blacklists.

Example

Display reference information about all STA blacklist profiles.

```
<HUAWEI> display sta-blacklist-profile all
------------------------------------------------------------
Profile name                    Reference
------------------------------------------------------------
sta-blacklist-profile1           1
------------------------------------------------------------
Total: 1
```

Table 11-223 Description of the **display sta-blacklist-profile all** command output

Item	Description
Profile name	Name of a STA blacklist profile.

Item	Description
Reference	Number of times a STA blacklist profile is referenced.

Display information about the STA blacklist profile **sta-blacklist-profile1**.

```
<HUAWEI> display sta-blacklist-profile name sta-blacklist-profile1
-------------------------------------------------------------
Index      MAC              Description
-------------------------------------------------------------
0          00e0-fc11-2222
-------------------------------------------------------------
Total: 1
```

Table 11-224 Description of the **display sta-blacklist-profile name** command output

Item	Description
Index	Blacklist index.
MAC	MAC address of a STA in the blacklist. To configure the parameter, run the **sta-mac** command.
Description	Description of a MAC address in the blacklist.

11.11.26 display station dynamic-blacklist

Function

The **display station dynamic-blacklist** command displays the dynamic blacklist on an AP.

Format

display station dynamic-blacklist { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays information about STAs that are denied access on the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
ap-name *ap-name*	Displays information about STAs that are denied access on the AP with a specified name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

There is a STA dynamic blacklist on an AP. The blacklist helps control access of STAs, for example, forbidding STAs with bogus IP addresses to go online. If a STA is not allowed to go online, the STA is added to the dynamic blacklist. Before the dynamic blacklist entry ages out, the STA cannot associate with the AP. After the aging time of a dynamic blacklist entry is reached, the dynamic blacklist entry is automatically deleted. During this period, if the STA on an entry is added to the blacklist again, the aging time of the entry is updated and recalculated.

The administrator can run this command to check STAs in the blacklist and the reasons for adding the STAs to the blacklist.

Example

Display the dynamic blacklist on AP.

```
<HUAWEI> display station dynamic-blacklist ap-name example
Total: 1
--------------------------------------------------------------------------------
STA MAC          Time left(s)   Reason
--------------------------------------------------------------------------------
00e0-fc12-3456   160            WIDS attack
--------------------------------------------------------------------------------
```

Table 11-225 Description of the **display station dynamic-blacklist** command output

Item	Description
STA MAC	MAC address of a STA.
Time left(s)	Remaining aging period, in seconds. To configure the parameter, run the **dynamic-blacklist aging-time** command.

Item	Description
Reason	Reason why a STA is added to the dynamic blacklist. ● static IP: The AP is configured to deny access of STAs with bogus IP addresses, and the STA has a static IP address configured. ● ARP flood: The AP is configured to detect and defend against ARP flood attacks, and the STA initiates an ARP flood attack. ● IGMP flood: The AP is configured to detect and defend against IGMP flood attacks, and the STA initiates an IGMP flood attack. ● ND flood: The AP is configured to detect and defend against ND flood attacks, and the STA initiates an ND flood attack. ● DHCP flood: The AP is configured to detect and defend against DHCP flood attacks, and the STA initiates a DHCP flood attack. ● DHCPv6 flood: The AP is configured to detect and defend against DHCPv6 flood attacks, and the STA initiates a DHCPv6 flood attack. ● MDNS flood: The AP is configured to detect and defend against mDNS flood attacks, and the STA initiates an mDNS flood attack. ● other multicast flood: The AP is configured to detect and defend against flood attacks through multicast packets other than IGMP, and mDNS multicast packets, and the STA initiates such an attack. ● other broadcast flood: The AP is configured to detect and defend against flood attacks through broadcast packets other than ARP, DHCP, DHCPv6, and ND multicast packets, and the STA initiates such an attack. ● WIDS attack: The AP is configured to detect attacks on a WLAN. ● MESH key fail: Key negotiation fails during mesh link setup.

Item	Description
	• other: Other reason

11.11.27 display sta-whitelist-profile

Function

The **display sta-whitelist-profile** command displays configuration and reference information about a STA whitelist profile.

Format

display sta-whitelist-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all STA whitelist profiles.	-
name *profile-name*	Displays information about a specified STA whitelist profile.	The STA whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a STA whitelist on a device, you can run this command to check whether a MAC address is in the whitelist.

Example

Display reference information about all STA whitelist profiles.

```
<HUAWEI> display sta-whitelist-profile all
------------------------------------------------------------
Profile name                    Reference
------------------------------------------------------------
sta-whitelist-profile1           1
------------------------------------------------------------
Total: 1
```


Table 11-226 Description of the **display sta-whitelist-profile all** command output

Item	Description
Profile name	Name of a STA whitelist profile.
Reference	Number of times a STA whitelist profile is referenced.

Display information about the STA whitelist profile **sta-whitelist-profile1**.

```
<HUAWEI> display sta-whitelist-profile name sta-whitelist-profile1
-------------------------------------------------------------
Index      MAC                Description
-------------------------------------------------------------
0          00e0-fc11-2222
-------------------------------------------------------------
Total: 1
-------------------------------------------------------------
Index      OUI                Description
-------------------------------------------------------------
0          00-00-01
-------------------------------------------------------------
Total: 1
```

Table 11-227 Description of the **display sta-whitelist-profile name** command output

Item	Description
Index	Whitelist index.
MAC	MAC address of a STA in the whitelist. To configure the parameter, run the **sta-mac** command.
OUI	OUI of a STA in the whitelist. To configure the parameter, run the **oui** command.
Description	Description of a MAC address in the whitelist.

11.11.28 display wlan ids attack-detected

Function

The **display wlan ids attack-detected** command displays information about the detected attacking devices.

Format

display wlan ids attack-detected { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all types of attacking devices.	-
flood	Displays information about devices launching flood attacks.	-
spoof	Displays information about devices launching spoofing attacks.	-
wapi-psk	Displays information about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Displays information about devices launching weak IV attacks.	-
wep-share-key	Displays information about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Displays information about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Displays information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Displays information about the detected attacking devices with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, you can run this command to view information about the attacking devices.

Prerequisites

The attack detection functions of all types have been enabled using the **wids attack detect enable** command.

Example

Display information about all current attacking devices.

```
<HUAWEI> display wlan ids attack-detected all
#AP: Number of monitor APs that have detected the device
AT: Last detected attack type
CH: Channel number
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  wiv: Weak IV detected
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      eapl: EAPOL logoff frame
saf: Spoofed disassociation frame
sdf: Spoofed deauthentication frame
otsf: Other types of spoofing frames
--------------------------------------------------------------------------------
MAC address     AT     CH   RSSI(dBm)  Last detected time     #AP
--------------------------------------------------------------------------------
00e0-fc02-9c81  pbr    165  -87        2014-11-20/15:51:13    1
00e0-fc76-03e9  pbr    165  -84        2014-11-20/15:52:13    1
00e0-fc74-691f  act    165  -67        2014-11-20/15:43:33    1
00e0-fcb7-171d  pbr    165  -88        2014-11-20/15:41:43    1
00e0-fcb7-171f  act    165  -87        2014-11-20/15:44:03    1
--------------------------------------------------------------------------------
Total: 5, printed: 5
```

Table 11-228 Description of the **display wlan ids attack-detected all** command output

Item	Description
MAC address	• For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. • For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
AT	Acronym of the attack type.
CH	Channel in which the last attack is detected.
RSSI(dBm)	Average received signal strength indicator (RSSI) of the attack frames detected.
Last detected time	Last time at which an attack was detected.

Item	Description
#AP	Number of APs which detect this attack.

Display information about the attacking device with a specified MAC address.

```
<HUAWEI> display wlan ids attack-detected mac-address 00e0-fc47-aad0
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  wiv: Weak IV detected
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      eapl: EAPOL logoff frame
saf: Spoofed disassociation frame
sdf: Spoofed deauthentication frame
otsf: Other types of spoofing frames
--------------------------------------------------------------------------------
MAC address                      : 00e0-fc47-aad0
Number of detected APs           : 1
Channel                          : 165
RSSI(dBm)                        : -80
Reported AP 1
  AP name                        : ap-13
  Flood attack type              : pbr
  First detected time(Flood)     : 2014-11-20/15:50:33
  Spoof attack type              : -
  First detected time(Spoof)     : -
  First detected time(Weak-iv)   : -
  First detected time(WEP)       : -
  First detected time(WPA)       : -
  First detected time(WPA2)      : -
  First detected time(WAPI)      : -
--------------------------------------------------------------------------------
```

Table 11-229 Description of the **display wlan ids attack-detected mac-address** *mac-address* command output

Item	Description
MAC address	• For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. • For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
Number of detected APs	Number of APs which detect this attack.
Channel	Channel in which the last attack is detected.
RSSI(dBm)	Average received signal strength indicator (RSSI) of the attack frames detected.

Item	Description
Reported AP	Information of the AP which detects the attack.
AP name	Name of the AP which detects the attack.
Flood attack type	Flood attacks detected by the AP.
Spoof attack type	Spoofing attacks detected by the AP.
First detected time	First time when an attack is detected by an AP.

11.11.29 display wlan ids attack-detected statistics

Function

The **display wlan ids attack-detected statistics** command displays the number of attacks detected.

Format

display wlan ids attack-detected statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, you can run the **display wlan ids attack-detected statistics** command to view the total number of all types of attacks.

Prerequisites

The attack detection functions of all types have been enabled using the **wids attack detect enable** command.

Example

Display the number of attacks detected.


```
<HUAWEI> display wlan ids attack-detected statistics
Attack tracking since: 2015-01-27/12:02:11
------------------------------------------------------------------------------
Type                                    Total
------------------------------------------------------------------------------
Probe request frame flood attack                : 0
Authentication request frame flood attack       : 0
Deauthentication frame flood attack             : 0
Association request frame flood attack          : 0
Disassociation request frame flood attack       : 0
Reassociation request frame flood attack        : 0
Action frame flood attack                       : 0
EAPOL start frame flood attack                  : 0
EAPOL logoff frame flood attack                 : 0
Weak IVs detected                               : 0
Spoofed deauthentication frame attack           : 0
Spoofed disassociation frame attack             : 0
Other types of spoofing frame attack            : 0
WEP share-key attack                            : 0
WPA attack                                      : 0
WPA2 attack                                     : 0
WAPI attack                                     : 0
------------------------------------------------------------------------------
```


Table 11-230 Description of the **display wlan ids attack-detected statistics** command output

Item	Description
Type	Attack type: • Probe request frame flood attack • Authentication request frame flood attack • Deauthentication frame flood attack • Association request frame flood attack • Disassociation request frame flood attack • Reassociation request frame flood attack • Action frame flood attack • EAPOL start frame flood attack • EAPOL logoff frame flood attack • Weak IVs detected • Spoofed deauthentication frame attack • Spoofed disassociation frame attack • Other types of spoofing frame attack • WEP share-key attack: brute force cracking attack in WEP-SK authentication mode • WPA attack: brute force cracking attack in WPA-PSK authentication mode • WPA2 attack: brute force cracking attack in WPA2-PSK authentication mode • WAPI attack: brute force cracking attack in WAPI authentication mode
Total	Total number of attacks detected.

11.11.30 display wlan ids attack-history

Function

The **display wlan ids attack-history** command displays historical records about the attacking devices detected.

Format

display wlan ids attack-history { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays historical records about all types of attacking devices.	-
flood	Displays historical records about devices launching flood attacks.	-
spoof	Displays historical records about devices launching spoofing attacks.	-
wapi-psk	Displays historical records about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Displays historical records about devices launching weak IV attacks.	-
wep-share-key	Displays historical records about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Displays historical records about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Displays information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Displays historical records about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, information about the detected attacking devices is saved in the attacking device list. If an attacking device no longer

launches an attack, the device is removed from the attacking device list and saved to the historical attacking device list. You can run the **display wlan ids attack-history** command to check historical records about the attacking devices detected.

Prerequisites

The attack detection functions of all types have been enabled using the **wids attack detect enable** command.

Example

Display historical records of all attacking devices.

```
<HUAWEI> display wlan ids attack-history all
act: Action frame             asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  wiv: Weak IV detected
pbr: Probe request            rar: Reassociation request
eaps: EAPOL start frame       eapl: EAPOL logoff frame
saf: Spoofed disassociation frame
sdf: Spoofed deauthentication frame
otsf: Other types of spoofing frames
AP: Name of the monitor AP that has detected the device
AT: Attack type               CH: Channel number
--------------------------------------------------------------------------------
MAC address     AT     CH   RSSI(dBm)  Last detected time    AP
--------------------------------------------------------------------------------
00e0-fc12-37ec  pbr    165  -86        2014-11-20/15:51:43   ap-13
00e0-fc12-171d  pbr    165  -88        2014-11-20/15:41:43   ap-13
00e0-fc12-0bf4  pbr    165  -81        2014-11-20/15:41:53   ap-13
--------------------------------------------------------------------------------
Total: 3, printed: 3
```

Table 11-231 Description of the **display wlan ids attack-history all** command output

Item	Description
MAC address	• For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. • For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
AT	Acronym of the attack type.
CH	Channel in which the last attack is detected.
RSSI(dBm)	Average received signal strength indicator (RSSI) of the attack frames detected.
Last detected time	Last time at which an attack is detected.
AP	Name of the monitor AP.

11.11.31 display wlan ids contain

Function

The **display wlan ids contain** command displays information about contained devices.

Format

display wlan ids contain { **all** | **ap** | **adhoc** | **client** | **ssid** | **mac-address** *mac-address* | **monitor-ap** { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Displays information about all contained devices.	-
ap	Displays information about contained APs.	-
adhoc	Displays information about contained ad-hoc devices.	-
client	Displays information about contained STAs.	-
ssid	Displays information about contained SSIDs.	-
mac-address *mac-address*	Displays information about the contained device with a specified MAC address.	The MAC address must exist.
monitor-ap ap-name *ap-name*	Displays information about contained devices that are detected by the AP with a specified name.	The AP name must exist.
monitor-ap ap-id *ap-id*	Displays information about contained devices that are detected by the AP with a specified ID.	The AP ID must exist.
monitor-ap { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*	Displays information about contained devices that are detected by the radio with a specified ID on a specified AP.	The radio ID must exist on the AP.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After WIDS or WIPS is enabled, you can run this command to view information about contained devices.

Example

Display the list of all contained devices.

```
<HUAWEI> display wlan ids contain all
#Rf: Number of monitor radios that have contained the device
CH: Channel number
--------------------------------------------------------------------------------
MAC address      CH  Authentication   Last detected time   #Rf   Reason   SSID
--------------------------------------------------------------------------------
00e0-fc12-3456   11  open            2014-11-20/16:16:57  1     manual     -
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-232 Description of the **display wlan ids contain all** command output

Item	Description
MAC address	MAC address of the contained device.
CH	Channel on which the monitor AP detected the contained device for the last time.
Authentication	Authentication mode of the contained device.
Last detected time	Last time at which the monitor AP detected the contained device.
#Rf	Number of monitor radios that have contained the device.
Reason	Reason for the device to be contained. The priorities of containment reasons are in descending order as follows: manual > open-encrypt > spoof-ap > protect-client > client > adhoc.
SSID	SSID of the contained device.

Display information about contained SSIDs.


```
<HUAWEI> display wlan ids contain ssid
#Dev: Number of devices using SSID
--------------------------------------------------------------------------------
 SSID                          #Dev     Last detected time
--------------------------------------------------------------------------------
 CMCC                           2       2012-07-27/16:41:55
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-233 Description of the **display wlan ids contain ssid** command output

Item	Description
SSID	Contained SSID.
#Dev	Number of devices that use the SSID.
Last detected time	Last time at which the device using the SSID was detected.

Display information about the contained device with a specified MAC address.

```
<HUAWEI> display wlan ids contain mac-address 00e0-fc12-3456
--------------------------------------------------------------------------------
MAC address                                  : 00e0-fc12-3456
BSSID                                       : 00e0-fc12-3456
Type                                        : rogue client
SSID                                        : -
Authentication                              : -
Number of monitor radios that have contained the device : 1
Last detected channel                        : 1
Maximum RSSI(dBm)                            : -54
Beacon interval(TUs)                         : 0
First detected time                         : 2015-10-20/15:06:26

Reported AP 1
 AP name                                    : admin_ap0_admin_ap0_admin
 Radio ID                                   : 0
 MAC address                                : 00e0-fc12-3455
 Radio type                                 : 802.11bg
 Channel                                    : 1
 RSSI(dBm)                                  : -54
 Last detected time                         : 2015-10-20/15:06:26
 Counter measure                            : Y
 Reason                                     : manual
--------------------------------------------------------------------------------
```

Table 11-234 Description of the **display wlan ids contain mac-address** command output

Item	Description
MAC address	MAC address of the detected device.
BSSID	BSSID of the detected device.
Type	Type of the detected device.
SSID	SSID of the detected device.

Item	Description
Authentication	Authentication mode of the detected device.
Number of monitor radios that have contained the device	Number of radios that contain the device. If WIDS is enabled on multiple APs, the type of the device may be contained by these APs' radios.
Last detected channel	Channel on which the device was detected for the last time.
Maximum RSSI(dBm)	Maximum RSSI of the detected device.
Beacon interval(TUs)	Interval at which the detected device sends Beacon frames.
First detected time	First time at which the device was detected.
Reported AP 1	Information about the monitor AP which reports detection information.
AP name	Name of the monitor AP.
Radio ID	Radio ID of the monitor AP.
MAC address	MAC address of the monitor AP.
Radio type	Radio type of the monitor AP.
Channel	Channel of the monitor AP.
RSSI(dBm)	RSSI of the monitor AP.
Last detected time	Last time when the device was detected.
Counter measure	Whether the device is contained.
Reason	Reason for the device to be contained. The priorities of containment reasons are in descending order as follows: manual > open-encrypt > spoof-ap > protect-client > client > adhoc.

```
<HUAWEI> display wlan ids contain monitor-ap ap-name example
Countermeasures Device Profile
--------------------------------------------------------------------------------
AP MAC address                    : 00e0-fc12-3456
AP type                         : xxxxxxx
AP name                           : example
Contain device 0
  MAC address                     : 00e0-fc12-3455
  BSSID                         : 00e0-fc12-3455
  Type                          : rogue client
```



```
SSID                                : -
Authentication                      : -
Last detected channel by this AP    : 1
Maximum RSSI(dBm)                   : -71
Beacon interval(TUs)                : 0
First detected time                 : 2015-10-20/15:06:26
Reason                              : manual
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-235 Description of the **display wlan ids contain monitor-ap** command output

Item	Description
AP MAC address	MAC address of the monitor AP.
AP type	Type of the monitor AP.
AP name	Name of the monitor AP.
MAC address	MAC address of the contained device.
BSSID	BSSID of the contained device.
Type	Type of the contained device.
SSID	SSID of the contained device.
Authentication	Authentication mode of the contained device.
Last detected channel by this AP	Channel on which the monitor AP detected the contained device for the last time.
Maximum RSSI(dBm)	Maximum RSSI of the contained device.
Beacon interval()	Interval at which the contained device sends Beacon frames.
First detected time	First time at which the device was detected.
Reason	Reason for the device to be contained. The priorities of containment reasons are in descending order as follows: manual > open-encrypt > spoof-ap > protect-client > client > adhoc.

11.11.32 display wlan ids device-detected

Function

The **display wlan ids device-detected** command displays various wireless devices detected on the WLAN.

Format

display wlan ids device-detected { **all** | [**interference** | **rogue**] **ap** | [**rogue**] **bridge** | [**rogue**] **client** [**bssid** *bssid*] | **adhoc** | [**rogue**] **ssid** | **mac-address** *mac-address* | **monitor-ap** { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Displays all wireless devices detected on the WLAN.	-
interference	Displays interfering devices detected on the WLAN.	-
rogue	Displays rogue devices detected on the WLAN.	-
ap	Displays APs detected on the WLAN.	-
bridge	Displays bridge devices detected on the WLAN.	-
client	Displays user terminals detected on the WLAN.	-
bssid *bssid*	Displays detailed information about devices with the specified BSSID detected on the WLAN.	The format is H-H-H. An H is a hexadecimal number of 4 digits.
adhoc	Displays detected user terminals that belong to the ad-hoc network on the WLAN.	-
ssid	Displays detailed information about devices with the specified SSID detected on the WLAN.	-
mac-address *mac-address*	Displays detailed information about the device with a specified MAC address detected on the WLAN.	The MAC address must exist.
monitor-ap ap-name *ap-name*	Displays detailed information about devices detected by the monitor AP with a specified name on the WLAN.	The AP name must exist.
monitor-ap ap-id *ap-id*	Displays detailed information about devices detected by the monitor AP with a specified ID on the WLAN.	The AP ID must exist.

Parameter	Description	Value
monitor-ap { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*	Displays detailed information about devices detected by the radio with a specified ID on a specified AP on the WLAN.	The radio ID must exist on the AP.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To ensure the WLAN reliability, all the wireless devices on the current WLAN must be monitored. You can run the **display wlan ids detected** command to view information about the wireless devices detected.

Prerequisites

The device detection function has been enabled on the AP using the **wids device detect enable** command.

Example

Display all wireless devices detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected all
Flags: r: rogue, p: permit, i: interference, a: adhoc, w: AP, b: wireless-bridge, c: client
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
--------------------------------------------------------------------------------------------
MAC address     Type    CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
--------------------------------------------------------------------------------------------
00e0-fc20-de2b  i/w     1   -60       5       open             2014-11-20/11:03:44  1     -
--------------------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-236 Description of the **display wlan ids device-detected all** command output

Item	Description
MAC address	MAC address of the detected device.

Item	Description
Type	Type of the detected device: • r: rogue device • p: authorized device • i: interfering device • a: user terminal on the ad-hoc network • w: AP • b: bridge device • c: user terminal
CH	Channel on which the device was detected for the last time.
RSSI(dBm)	RSSI of the detected device.
StaNum	Number of STAs associated with the detected device.
Authentication	Authentication mode of the detected device.
Last detected time	Last time when the device was detected.
#Rf	Number of radios that detect the device.
SSID	SSID of the detected device.

Display information about APs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected ap
Flags: r: rogue, p: permit, i: interference
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
--------------------------------------------------------------------------------
MAC address     Type  CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
--------------------------------------------------------------------------------
00e0-fc20-de2b  r     1   -60       5       open             2014-11-20/11:03:44  1     -
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display information about rogue APs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected rogue ap
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
--------------------------------------------------------------------------------
MAC Address     CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
--------------------------------------------------------------------------------
00e0-fc20-de2b  1   -60       5       open             2014-11-20/11:03:44  1     -
```



```
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display information about interference APs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected interference ap
Flags: r: rogue, p: permit, i: interference
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
--------------------------------------------------------------------------------
MAC address     Type  CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
--------------------------------------------------------------------------------
00e0-fc20-de2b  i     1   -60       5       open             2014-11-20/11:03:44  1     -
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display information about ad-hoc devices detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected adhoc
Flags: r: rogue
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
--------------------------------------------------------------------------------
MAC address     Type  CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
--------------------------------------------------------------------------------
00e0-fc20-de2d  r     6   -60       -       -                2014-11-20/11:12:58  2     -
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display information about SSIDs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected ssid
#Dev: Number of devices using SSID
--------------------------------------------------------------------------------
SSID                          #Dev  Last detected time
--------------------------------------------------------------------------------
trad                          1     2014-11-20/11:01:44
CMCC-4G                       6     2014-11-20/11:14:13
--------------------------------------------------------------------------------
Total: 2, printed: 2
```

Table 11-237 Description of the **display wlan ids device-detected ssid** command output

Item	Description
SSID	SSID detected.
#Dev	Number of devices that use the SSID.
Last detected time	Last time at which the device using the SSID was detected.

Display information about spoofing SSIDs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected rogue ssid
#Dev: number of devices using rogue SSID
--------------------------------------------------------------------------------
Rogue SSID  Spoof profile  #Dev  Last detected time
            Pattern rule
--------------------------------------------------------------------------------
```



```
ao          a0              1     2014-11-20/11:14:39
            ao
al          a1              2     2014-11-20/11:14:39
            al
--------------------------------------------------------------------------------
ssid        --              1     2014-11-20/15:59:45
--------------------------------------------------------------------------------
Total: 3
```

Table 11-238 Description of the **display wlan ids device-detected rogue ssid** command output

Item	Description
Rogue SSID	Spoofing SSIDs detected, including SSIDs same as the authorized SSIDs and SSIDs matching the specified fuzzy rules.
Spoof profile	WIDS spoof SSID profile owned the fuzzy matching rule.
Pattern rule	Fuzzy matching rule for the spoofing SSID.
#Dev	Number of APs using the SSID.
Last detected time	Last time when the SSID was detected.

Display detailed information about the device with the MAC address 00e0-fce9-1c00 detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected mac-address 00e0-fce9-1c00
Detected MAC List
--------------------------------------------------------------------------------
MAC address                                    : 00e0-fce9-1c00
BSSID                                          : 00e0-fce9-1c00
Type                                           : rogue ap
SSID                                           : -
Authentication                                 : 802.1x
Number of monitor radios that have detected the device  : 1
Last detected channel                          : 1
Maximum RSSI(dBm)                              : -80
Beacon interval(TUs)                           : -
First detected time                            : 2015-10-20/15:07:23
Reported AP 1
 AP name                                       : admin_ap0_admin_ap0_admin
 Radio ID                                      : 0
 MAC address                                   : 00e0-fc1e-c4a0
 Radio type                                    : 802.11bg
 Channel                                       : 1
 RSSI(dBm)                                     : -80
 Last detected time                            : 2015-10-20/15:07:23
 Counter measure                               : Y
 Counter measure reason                        : spoof-ssid-ap
--------------------------------------------------------------------------------
```


Table 11-239 Description of the **display wlan ids device-detected mac-address** command output

Item	Description
MAC address	MAC address of the detected device.
BSSID	BSSID of the detected device.
Type	Type of the detected device.
SSID	SSID of the detected device.
Authentication	Authentication mode of the detected device.
Number of monitor radios that have detected the device	Number of radios that detect the device. If WIDS is enabled on multiple APs, the type of the device may be detected by these APs' radios.
Last detected channel	Channel of the detected device.
Maximum RSSI(dBm)	Maximum RSSI of the detected device.
Beacon interval(TUs)	Interval at which the detected device sends Beacon frames.
First detected time	First time at which the device was detected.
Reported AP 1	Information about the monitor AP which reports detection information.
AP name	Name of the monitor AP.
Radio ID	Radio ID of the monitor AP.
MAC address	MAC address of the monitor AP.
Radio type	Radio type of the monitor AP.
Channel	Channel of the monitor AP.
RSSI(dBm)	RSSI of the monitor AP.
Last detected time	Last time when the device was detected.
Counter measure	Whether the device is contained.

Item	Description
Counter measure reason	Reason why the device is contained. • open-encrypt: The authentication mode of the device is open. • spoof-ssid-ap: The device is a rogue AP or interference AP with a spoofing SSID. • protect-client: The device is a STA in the STA whitelist and is contained to prevent it from accessing a rogue AP. • client: The device is a rogue STA or interference STA. • adhoc: The device is an ad-hoc device. • manual: The device is manually contained.

11.11.33 display wlan ids device-detected statistics

Function

The **display wlan ids device-detected statistics** command displays statistics on all wireless devices detected on a WLAN.

Format

display wlan ids device-detected statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan ids device-detected statistics** command to view statistics on all wireless devices detected on a WLAN.

Example

Display statistics on wireless devices detected on a WLAN.

```
<HUAWEI> display wlan ids device-detected statistics
-------------------------------------------------------------------------------------------

Rogue Adhoc          : 0
Contain Adhoc        : 0
Rogue AP             : 0
Permit AP            : 0
Interference AP      : 0
Contain AP           : 0
Rogue client         : 2
Permit client        : 0
Interference Client  : 0
Contain client       : 2
Permit Bridge        : 2
Rogue Bridge         : 0
Interference Bridge  : 0
-------------------------------------------------------------------------------------------
```

Table 11-240 Description of the **display wlan ids device-detected statistics** command output

Item	Description
Rogue Adhoc	Number of rogue ad-hoc devices.
Contain Adhoc	Number of contained ad-hoc devices.
Rogue AP	Number of rogue APs.
Permit AP	Number of authorized APs.
Interference AP	Number of interfering APs.
Contain AP	Number of contained APs.
Rogue Client	Number of rogue terminal devices.
Permit Client	Number of authorized terminal devices.
Interference Client	Number of interfering terminal devices.
Contain Client	Number of contained terminal devices.
Permit Bridge	Number of authorized bridge devices.
Rogue Bridge	Number of unauthorized bridge devices.
Interference Bridge	Number of interfering bridge devices.

11.11.34 display wlan dynamic-blacklist

Function

The **display wlan dynamic-blacklist** command displays information about devices in the dynamic blacklist.

Format

display wlan dynamic-blacklist { **all** | **ap-id** *ap-id* | **ap-name** *ap-name* | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all devices in the dynamic blacklist.	-
ap-id *ap-id*	Displays information about attacking devices detected by the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about attacking devices detected by the AP with a specified name.	The AP name must exist.
mac-address *mac-address*	Displays information about attack devices with a specified MAC address.	The MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An AP uses attack detection and dynamic blacklist functions to add a detected attack device to the dynamic blacklist, and rejects packets sent from this device until the device entry in the dynamic blacklist ages. You can run this command to view information about devices in the dynamic blacklist.

Example

Display information about all devices in the dynamic blacklist.

```
<HUAWEI> display wlan dynamic-blacklist all
#AP: Number of monitor APs that have detected the device
```



```
LAT: Left aging time(s)
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  eapl: EAPOL logoff frame
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      sti: Static IP
brf: Broadcast flood
--------------------------------------------------------------------------------
MAC address      Last detected time    Reason   #AP   LAT
--------------------------------------------------------------------------------
00e0-fc12-3451   2015-07-27/12:51:25   brf       1    100
00e0-fc12-3452   2015-07-27/12:51:25   pbr       1    200
00e0-fc12-3453   2015-07-27/12:51:25   pbr       1    200
00e0-fc12-3454   2015-07-27/12:51:25   sti       1    200
00e0-fc12-3455   2015-07-27/12:51:25   pbr       1    200
00e0-fc12-3456   2015-07-27/12:51:25   pbr       1    200
--------------------------------------------------------------------------------
Total: 6, printed: 6
```

Table 11-241 Description of the **display wlan dynamic-blacklist all** command output

Item	Description
MAC address	MAC address of the device in the dynamic blacklist.
Last detected time	Latest time when the device was added to the dynamic blacklist.
Reason	Reason why the device is added to the dynamic blacklist.
#AP	Number of APs that have detected and added the device to the dynamic blacklist.
LAT	Remaining aging time for the device in the dynamic blacklist.

Display information about all devices added to the dynamic blacklist by the AP named **wcw**.

```
<HUAWEI> display wlan dynamic-blacklist ap-name wcw
LAT: Left aging time(s)
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  eapl: EAPOL logoff frame
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      sti: Static IP
brf: Broadcast flood
--------------------------------------------------------------------------------
MAC address      Last detected time    Reason   LAT
--------------------------------------------------------------------------------
00e0-fc12-3451   2015-07-27/12:51:25   sti     100
00e0-fc12-3452   2015-07-27/12:51:25   brf     200
00e0-fc12-3453   2015-07-27/12:51:30   pbr     200
00e0-fc12-3454   2015-07-27/12:51:25   pbr     300
--------------------------------------------------------------------------------
Total: 4, printed: 4
```

Display information about specified devices in the dynamic blacklist.


```
<HUAWEI> display wlan dynamic-blacklist mac-address 00e0-fc12-3454
LAT: Left aging time(s)       BT: Block time(s)
act: Action frame             asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  eapl: EAPOL logoff frame
pbr: Probe request            rar: Reassociation request
eaps: EAPOL start frame       sti: Static IP
brf: Broadcast flood
------------------------------------------------------------
AP name  Last detected time    Reason   LAT     BT
------------------------------------------------------------
wcw      2015-07-27/12:51:25   pbr     100     900
wcw2     2015-07-27/12:51:25   pbr     100     1900
------------------------------------------------------------
Total: 2, printed: 2
```

Table 11-242 Description of the **display wlan dynamic-blacklist mac-address** command output

Item	Description
AP name	Name of the monitoring AP.
Last detected time	Last time when the device was detected.
Reason	Reason why the device is added to the dynamic blacklist.
LAT	Remaining aging time for the device in the dynamic blacklist.
BT	Duration for which the device is in the dynamic blacklist.

11.11.35 display wlan ids rogue-history

Function

The **display wlan ids rogue-history** command displays historical records of rogue devices.

Format

display wlan ids rogue-history { **all** | **ap** | **bridge** | **client** | **adhoc** | **ssid** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays historical records of all rogue devices.	-
ap	Displays historical records of rogue APs.	-

Parameter	Description	Value
bridge	Displays historical records of rogue bridge devices.	-
client	Displays historical records of rogue user terminals.	-
adhoc	Displays historical records of rogue ad-hoc devices.	-
ssid	Displays historical records of contained devices with unauthorized SSIDs.	-
mac-address *mac-address*	Displays historical records of devices with specified MAC addresses.	The MAC addresses must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display wlan ids rogue-history** command to view the historical records of rogue devices.

Prerequisites

The device detection function has been enabled on the AP using the **wids device detect enable** command.

Example

Display historical records of all rogue devices.

```
<HUAWEI> display wlan ids rogue-history all
Flags: a: adhoc, w: AP, b: wireless-bridge, c: client
CH: Channel number
------------------------------------------------------------------------------
MAC address     Type  CH  Authentication   Last detected time   SSID
------------------------------------------------------------------------------
00e0-fc12-3456  w     11  open             2014-11-20/11:20:37  wlan
00e0-fc12-3457  c     11  -                2014-11-20/11:16:07  -
------------------------------------------------------------------------------
Total: 2, printed: 2
```


Table 11-243 Description of the **display wlan ids rogue-history all** command output

Item	Description
MAC address	MAC address of the rogue device listed in the historical record list.
Type	Type of the rogue device listed in the historical record list: ● a: user terminal on the ad-hoc network ● w: AP ● b: bridge device ● c: user terminal
CH	Channel in which the device is detected for the last time.
Authentication	Authentication mode of the rogue device listed in the historical record list.
Last detected time	Last time when the device is detected.
SSID	SSID of the detected device.

Display historical records of rogue APs.

```
<HUAWEI> display wlan ids rogue-history ap
CH: channel number
--------------------------------------------------------------------------------
MAC address     CH  Authentication   Last detected time   SSID
--------------------------------------------------------------------------------
00e0-fc12-3458  11  open             2014-11-20/11:20:37  wlan
00e0-fc12-3459  11  open             2014-11-20/11:20:44  -
--------------------------------------------------------------------------------
Total: 2, printed: 2
```

Display historical records of SSIDs.

```
<HUAWEI> display wlan ids rogue-history ssid
#Dev: number of devices using SSID
--------------------------------------------------------------------------------
SSID                          #Dev  Last detected time
--------------------------------------------------------------------------------
trad                          1     2014-11-20/11:01:44
CMCC-4G                       6     2014-11-20/11:14:13
X+Z_007                       1     2014-11-20/11:20:15
tntjoyo                       1     2014-11-20/11:18:42
--------------------------------------------------------------------------------
Total: 4, printed: 4
```


Table 11-244 Description of the **display wlan ids rogue-history ssid** command output

Item	Description
SSID	SSID of the detected device.
#Dev	Number of devices that use the SSID.
Last detected time	Last time at which the device using the SSID is detected.

Display historical records of an AP or STA with a specified MAC address.

```
<HUAWEI> display wlan ids rogue-history mac-address 00e0-fc03-0206
------------------------------------------------------------------------------
MAC address                 : 00e0-fc03-0206
SSID                      : wlan
Type                      : rogue ap
Authentication              : 802.1x
Last detected time          : 2012-10-25/09:22:29
------------------------------------------------------------------------------
```

Table 11-245 Description of the **display wlan ids rogue-history mac-address** command output

Item	Description
MAC address	MAC address of the detected device.
Type	Type of the detected device.
SSID	SSID of an ESS.
Authentication	Authentication mode of the detected device.
Last detected time	Last time when the device is detected.

11.11.36 display wlan ids spoof-ssid fuzzy-match

Function

The **display wlan ids spoof-ssid fuzzy-match** command displays fuzzy matching rules for spoofing SSIDs.

Format

display wlan ids spoof-ssid fuzzy-match regex *regex-value*

Parameters

Parameter	Description	Value
regex *regex-value*	Specifies the matching rules for spoofing SSIDs and displays spoofing SSIDs that match the rules.	The rules must exist. The value is in text format and can contain 1 to 48 case-sensitive characters. It supports Chinese characters or mixture of Chinese and English characters. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view SSIDs that match a specific rule, run the **display wlan ids spoof-ssid fuzzy-match regex** *regex-value* command.

Example

Display SSIDs that match a specific rule.

```
<HUAWEI> display wlan ids spoof-ssid fuzzy-match regex ^HUAWE[1l]$
#Dev: Number of devices using SSID
--------------------------------------------------------------------------------
Match SSID                      #Dev  Last detected time   WIDS spoof profile
--------------------------------------------------------------------------------
HUAWE1                           2    2014-03-06/12:44:37  example
HUAWEl                           1    2014-03-06/12:44:50  example
--------------------------------------------------------------------------------
Total: 2
```


Table 11-246 Description of the **display wlan ids spoof-ssid fuzzy-match regex** command output

Item	Description
Match SSID	SSID matching a specific rule.
#Dev	Number of APs using the matching SSID.
Last detected time	Latest time when the SSID is detected.
WIDS spoof profile	WIDS spoof profile to which the rules belong.

11.11.37 display wlan wapi certificate

Function

The **display wlan wapi certificate** command displays the content of a certificate file.

Format

display wlan wapi certificate file-name *file-name*

Parameters

Parameter	Description	Value
file-name *file-name*	Specifies a certificate file name.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) and cannot start or end with double quotation marks (" ") or spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view content of certificate files imported to the device.

In the command, *file-name* must specify the complete path of a certificate file. For example, if the certificate file **as.cer** is saved in the flash memory, run **display wlan wapi certificate file-name flash:/as.cer** command.

Example

Display content of certificate file **as.cer**.

```
<HUAWEI> display wlan wapi certificate file-name flash:/as.cer
Certificate:
Data:
  Version: V3
  Serial number:
     50 FA CF CA
  Signature algorithm: sha256ECDSA192
  Issuer:
     C = CN
     O = 0003
     OU = CUCC
     CN = as_test_1@ASU
  Validity:
    Not before: 2013-01-19 16:54:34 UTC
    Not after : 2033-01-19 16:54:34 UTC
  Subject:
     C = CN
     O = 0003
     OU = CUCC
     CN = as_test_1@ASU
  Subject public key information:
    Public key algorithm: ECC
    Public key: (392 bit)
     04 31 AB F2 76 AE E4 BD EF E6 ED CA 93 C0 04 C8
     C9 C9 BF 6F A3 6A F9 A1 9E 35 3E 9B 08 21 EF 20
     5E 82 C1 42 2D A9 42 C3 CE 91 98 7F 21 83 7C 71
     3A
```

Table 11-247 Description of the **display wlan wapi certificate** command output

Item	Description
Version	Version of the X.509 certificate.
Serial number	Serial number of the certificate.
Signature algorithm	Signature algorithm used by the certificate.
Issuer	Certificate issuer.
Validity	Valid period of the certificate, specified by the start date and end date.
Subject	Subject of the certificate.
Subject public key information	Information about the public key of the certificate.

11.11.38 dynamic-blacklist aging-time

Function

The **dynamic-blacklist aging-time** command sets an aging time for a dynamic blacklist.

The **undo dynamic-blacklist aging-time** command restores the aging time of a dynamic blacklist to the default value.

By default, the aging time of a dynamic blacklist is 300 seconds.

Format

dynamic-blacklist aging-time *time*

undo dynamic-blacklist aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time at the expiry of which a specified MAC address is removed from the dynamic blacklist.	The value is an integer that ranges from 180 to 3600, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When detecting attacks from a STA, an AP reports the STA to the AC, forbids the STA to go online, and rejects any packets sent from the STA. As long as the STA is blacklisted, it cannot go online again even if it no longer launches attacks. To avoid that, you can run the **dynamic-blacklist aging-time** command to configure an aging time for the dynamic blacklist. If the configured aging time expires and the AP detects no attack from the STA, the STA is once again allowed to go online.

Example

Set the aging time of the dynamic blacklist to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] dynamic-blacklist aging-time 200
```


11.11.39 dynamic-blacklist disable

Function

The **dynamic-blacklist disable** command disables the dynamic blacklist function.

The **undo dynamic-blacklist disable** command enables the dynamic blacklist function.

By default, the dynamic blacklist function is enabled.

Format

dynamic-blacklist disable

undo dynamic-blacklist disable

Parameters

None

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attack detection is enabled to detect flood attacks, weak IV attacks, spoofing attacks, and brute force key cracking attacks. When detecting attacks initiated by a device, an AP reports an alarm to the AC. In addition, you can run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function on the AC for handling flood attacks and brute force key cracking attacks. The AC then automatically adds the attacking device to a dynamic blacklist and discards packets sent from the attacking device till the dynamic blacklist ages out.

An AP can use the dynamic blacklist to filter out the blacklisted wireless devices to avoid malicious attacks.

Follow-up Procedure

Run the **dynamic-blacklist aging-time** command to set an aging time for the dynamic blacklist.

Example

Enable the dynamic blacklist function.

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



```
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] undo dynamic-blacklist disable
```

11.11.40 flood-detect interval

Function

The **flood-detect interval** command sets the flood attack detection interval.

The **undo flood-detect interval** command restores the default flood attack detection interval.

By default, the flood attack detection interval is 10 seconds.

Format

flood-detect interval *interval*

undo flood-detect interval

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for flood attack detection.	The value is an integer that ranges from 10 to 120, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A flood attack occurs when an AP receives a large number of packets of the same type within a short period. As a result, the AP is flooded by too many attack packets to process service packets from authorized wireless terminals.

After the flood attack detection function is enabled, an AP counts the number of packets of the same type that it receives from a user at regular intervals. When the number exceeds a specified threshold, the AP considers that the user launches a flood attack. If the dynamic blacklist function is enabled, the user will be added to a dynamic blacklist.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the flood attack detection interval to 120s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect flood enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] flood-detect interval 120
```

11.11.41 flood-detect quiet-time

Function

The **flood-detect quiet-time** command sets the quiet time for an AP to report the detected flood attacks to the AC.

The **undo flood-detect quiet-time** command restores the quiet time for an AP to report the detected flood attacks to the AC.

By default, the quiet time is 600 seconds for an AP to report the detected flood attacks to the AC.

Format

flood-detect quiet-time *quiet-time-value*

undo flood-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report the detected flood attacks to the AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repeated alarms are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the quiet time to 300 seconds for an AP to report the detected flood attacks to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect flood enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] flood-detect quiet-time 300
```

11.11.42 flood-detect threshold

Function

The **flood-detect threshold** command sets the flood attack detection threshold. A flood attack occurs when an AP receives a large number of packets of the same type within a short period.

The **undo flood-detect threshold** command restores the default flood attack detection threshold.

By default, the flood attack detection threshold is 500.

Format

flood-detect threshold *threshold*

undo flood-detect threshold

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the flood attack detection threshold.	The value is an integer that ranges from 1 to 1000.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A flood attack occurs when a device receives a large number of packets of the same type within a short period. As a result, the device is flooded by too many attack packets to process service packets from authorized wireless terminals.

After the flood attack detection function is enabled, a device counts the number of packets of the same type that it receives from a user at regular intervals. When the number exceeds a specified threshold, the device considers that the user launches a flood attack. If the dynamic blacklist function is enabled, the user will be added to a dynamic blacklist. If the threshold is set to a small value, the device may incorrectly add authorized users to the dynamic blacklist, causing the users unable to go online.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the flood attack detection threshold to 350.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect flood enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] flood-detect threshold 350
```


11.11.43 ip source check user-bind enable

Function

The **ip source check user-bind enable** command enables IP source guard (IPSG) on APs.

The **undo ip source check user-bind enable** command disables IPSG on APs.

By default, IPSG is disabled on APs.

Format

ip source check user-bind enable

undo ip source check user-bind enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Users can configure static IP addresses for their clients and connect to the Internet after passing 802.1X authentication. To defend against source IP address spoofing attacks, you need to enable IPSG on APs.

To prevent IP packets of unauthorized users from entering external networks through an AP, enable IPSG in a VAP profile and bind the VAP profile to an AP or AP group. The IPSG function can filter incoming packets on an AP radio interface, preventing unauthorized packets from passing through the AP.

Example

Enable IPSG on APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] ip source check user-bind enable
```

11.11.44 learn-client-address dhcp-strict

Function

The **learn-client-address dhcp-strict** command enables strict STA IP address learning through DHCP.

The **undo learn-client-address dhcp-strict** command disables strict STA IP address learning through DHCP.

By default, strict STA IP address learning through DHCP is disabled.

Format

learn-client-address dhcp-strict [**blacklist enable**]

undo learn-client-address dhcp-strict

Parameters

Parameter	Description	Value
blacklist enable	Adds STAs with bogus IP addresses to a blacklist. By default, STAs with bogus IP addresses are not added to a blacklist.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA associates with an AP, the following situation occurs after strict STA IP address learning through DHCP is enabled:

- If the STA obtains an IP address through DHCP, the AP will automatically report the IP address to the AC. The STA IP address can be used to maintain the mapping between STA IP addresses and MAC addresses.
- For a STA using a static IP address:
  - If **blacklist enable** is specified, the STA will be added to a dynamic blacklist of the AP and cannot associate with the AP before the blacklist entry ages.
  - If **blacklist enable** is not specified, the STA can associate with the AP but the AP does not learn the IP address of the STA.

Prerequisites

STA address learning has been enabled using the **undo learn-client-address ipv4 disable** command.

Precautions

After strict STA IP address learning is enabled, it is recommended that you run the **ip source check user-bind enable** and **arp anti-attack check user-bind enable**

commands to enable IPSG and DAI so that STAs can communicate with the network only after obtaining an IP address through DHCP.

If this function is disabled, you can manually configure a static IP address. However, if a STA obtains an IP address dynamically using DHCP, goes online, and then is assigned a static IP address, the administrator cannot detect the IP address change of this STA.

Example

Enable strict STA IP address learning through DHCP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] learn-client-address dhcp-strict
```

11.11.45 learn-client-address { dhcpv6-strict | dhcpv6-slaac }

Function

The **learn-client-address { dhcpv6-strict | dhcpv6-slaac }** command enables strict STA IPv6 address learning.

The **undo learn-client-address { dhcpv6-strict | dhcpv6-slaac }** command disables strict STA IPv6 address learning.

By default, strict STA IPv6 address learning is disabled.

Format

learn-client-address { **dhcpv6-strict** | **dhcpv6-slaac** } [**blacklist enable**]

undo learn-client-address { **dhcpv6-strict** | **dhcpv6-slaac** }

Parameters

Parameter	Description	Value
dhcpv6-strict	Enables the STA IPv6 address learning function only through DHCPv6.	-
dhcpv6-slaac	Enables the STA IPv6 address learning function only through DHCPv6 or SLAAC in DHCPv6 + SLAAC scenarios.	-
blacklist enable	Adds STAs with bogus IPv6 addresses to a blacklist. By default, STAs with bogus IPv6 addresses are not added to a blacklist.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA associates with an AP, the following situation occurs after strict STA IPv6 address learning is enabled:

- If the STA obtains an IPv6 address through DHCPv6 or SLAAC, the AP will proactively report the STA's IPv6 address to the AC to maintain the STA's IPv6 address and MAC address binding entry.
- For a STA using a static IPv6 address:
  - If **blacklist enable** is specified, the STA will be added to a dynamic blacklist of the AP and cannot associate with the AP before the blacklist entry ages.
  - If **blacklist enable** is not specified, the STA can associate with the AP but the AP does not learn the IPv6 address of the STA.

Prerequisites

The ND trusted interface of the AP has been disabled using the **undo nd trust port** command in the VAP profile view.

STA address learning has been enabled using the **undo learn-client-address ipv6 disable** command.

Precautions

After strict STA IP address learning is enabled, it is recommended that you run the **ip source check user-bind enable** and **arp anti-attack check user-bind enable** commands to enable IPSG and DAI so that STAs can communicate with the network only after obtaining an IPv6 address.

If this function is disabled, you can manually configure a static IP address. However, if a STA obtains an IP address dynamically using DHCPv6 or SLAAC, goes online, and then is assigned a static IP address, the administrator cannot detect the IP address change of this STA.

If you run this command multiple times, only the latest configuration takes effect.

Example

Enable strict STA IPv6 address learning only through DHCPv6 or SLAAC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] learn-client-address dhcpv6-slaac
```

11.11.46 learn-client-address disable (VAP profile view)

Function

The **learn-client-address disable** command disables STA address learning.

The **undo learn-client-address disable** command enables STA address learning.

By default, STA address learning is enabled.

Format

learn-client-address { **ipv4** | **ipv6** } **disable**

undo learn-client-address { **ipv4** | **ipv6** } **disable**

Parameters

Parameter	Description	Value
ipv4	Indicates the IPv4 address.	-
ipv6	Indicates the IPv6 address.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a STA is associated with a STA address learning-enabled AP and obtains an IP address, the AP proactively reports the STA's IP address to the AC to maintain the IP address-MAC address binding entry of the STA. In addition, when a STA requests an IP address using DHCP, the AP can learn the IPv4 address of the STA gateway.

Prerequisites

- Before enabling STA address learning, ensure that the ND trusted interface of the AP for the IPv6 address has been disabled using the **undo nd trust port** command.
- Before disabling STA address learning, ensure that strict STA IPv4 address learning has been disabled using the **undo learn-client-address dhcp-strict** command and strict STA IPv6 address learning disabled using the **undo learn-client-address dhcpv6-strict** command.

Precautions

- The device enabled with STA address learning can learn only a limited number of IPv6 addresses; therefore, you are advised to configure only one IPv6 prefix for the IPv6 gateway. If you configure too many IPv6 prefixes, the number of IPv6 addresses exceeds the upper limit, and extra IPv6 addresses cannot be learned by the device. IPv6 addresses that are not learned by the device cannot be used for communication.

- If a bridging device functions as a STA to connect to an AP enabled with STA address learning, the AP cannot learn IP addresses of users connected to the bridging device; therefore, the users cannot communicate with the network. In this situation, disable STA address learning.
- Disabling STA address learning will lead to a Portal authentication failure.
- When a STA requests an IP address using DHCP, the STA address learning-enabled AP can only learn the IPv4 gateway address but cannot learn the IPv6 gateway address.
- If no STA connected to a STA address learning-enabled AP requests an IP address using DHCP, the AP cannot learn the gateway IP address.

Example

Disable STA IPv4 address learning.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] learn-client-address ipv4 disable
```

11.11.47 nd trust port

Function

The **nd trust port** command enables the ND trusted interface on an AP.

The **undo nd trust port** command cancels the configuration.

By default, the ND trusted interface is disabled on an AP

Format

nd trust port

undo nd trust port

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a bogus ND server is deployed at the user side, STAs may obtain incorrect IPv6 addresses and network configuration parameters and cannot communicate

properly. After the **undo nd trust port** command is executed in the VAP profile view, an AP discards the ND OFFER, ACK, and NAK packets sent by the bogus ND server and the IPv6 address of the unauthorized ND server.

Before WLAN services are delivered to an AP, run the **nd trust port** command in the AP wired port profile view. After the command is run, the AP receives the ND OFFER, ACK, and NAK packets sent by the authorized ND server and forwards the packets to STAs so that the STAs can obtain valid IPv6 addresses and go online.

Prerequisites

The function of processing STA IPv6 services has been enabled using the **sta-ipv6-service enable** command.

Before enabling the ND trusted interface, ensure that STA IPv6 address learning has been disabled using the **learn-client-address ipv6 disable** command.

Example

Create the VAP profile **vap1** and enable the ND trusted interface on the AP in the VAP profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] nd trust port
```

11.11.48 oui

Function

The **oui** command configures an organizationally unique identifier (OUI) for STAs in the whitelist.

The **undo oui** command deletes the OUI of a specified STA or all STAs in the whitelist.

By default, no OUI is configured for STAs in the whitelist.

Format

oui *oui* [**description** *description*]

undo oui { *oui* | **all** }

Parameters

Parameter	Description	Value
oui	Specifies the OUI of STAs in the whitelist.	The value is in H-H-H format. An H is a hexadecimal number of 2 digits. For example, **11-22-33** indicates a STA whose first 6 bits of the MAC address are 11-22-33.
description	Specifies the OUI description of STAs in the whitelist.	The value is a string of 1 to 80 characters.
all	Deletes the OUI of all STAs in the whitelist.	-

Views

STA whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

After the whitelist function is enabled, all STAs in the whitelist can connect to the WLAN. In some scenarios, all STAs with a specified OUI need to be added to the whitelist. You can run the **oui** command to add STAs with a specified OUI to the whitelist.

Example

Configure the OUI **00-11-22** for STAs in the whitelist profile **sta-whitelist-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-whitelist-profile name sta-whitelist-profile1
[HUAWEI-wlan-whitelist-prof-sta-whitelist-profile1] oui 00-11-22
```

11.11.49 permit-ap

Function

The **permit-ap** command configures a WIDS whitelist.

The **undo permit-ap** command deletes entries in the WIDS whitelist.

By default, no WIDS whitelist is configured.

Format

permit-ap { **mac-address** *mac-address* | **oui** *oui* | **ssid** *ssid* }

undo permit-ap { **mac-address** { *mac-address* | **all** } | **oui** { *oui* | **all** } | **ssid** { **name** *ssid* | **all** } }

Parameters

Parameter	Description	Value
mac-address *mac-address*	Adds or deletes an authorized MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
mac-address all	Deletes an authorized MAC address list.	-
oui *oui*	Adds or deletes an authorized OUI.	The value is in H-H-H format. An H is a hexadecimal number of 2 digits.
oui all	Deletes an authorized OUI list.	-

Parameter	Description	Value
ssid name *ssid*	Deletes an authorized SSID.	The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters. To start an SSID with a space, you need to encompass the SSID with double quotation marks (" "), for example, **" hello"**. The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to add a backslash (\) before the double quotation mark, for example, **\"hello**. The backslash occupies one character.

Parameter	Description	Value
ssid *ssid*	Adds an authorized SSID.	The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters. To start an SSID with a space, you need to encompass the SSID with double quotation marks (" "), for example, **" hello"**. The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to add a backslash (\) before the double quotation mark, for example, **\"hello**. The backslash occupies one character.
ssid all	Deletes an authorized SSID list.	-

Views

WIDS whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After WIDS/WIPS is enabled, rogue APs can be detected and contained. However, there may be APs of other vendors or other networks working in the existing signal coverage areas. If these APs are contained, their services will be affected. To prevent this situation, configure an authorized AP list, including an authorized MAC address list, OUI list, and SSID list. If a rogue AP is detected but matches the

authorized AP list, the AP is considered an authorized AP and will not be contained.

For example, APs of other vendors are deployed on the existing WLAN to expand network capacity. To prevent the APs from being contained, add OUIs of the vendors to a whitelist and add SSIDs of these APs to a whitelist. In this way, the device will consider the APs as authorized APs.

The device determines whether a detected AP is authorized as follows:

1. Check whether the AP's MAC address is in the authorized MAC address list.
   - If so, the AP is an authorized AP.
   - If not, go to step 2.
2. Check whether the AP's OUI and SSID are in the OUI and SSID lists.
   - If only the SSID is configured, check whether the AP's SSID is in the authorized SSID list.
     - If so, the AP is an authorized AP.
     - If not, the AP is a rogue AP.
   - If only the OUI is configured, check whether the AP's OUI is in the authorized OUI list.
     - If so, the AP is an authorized AP.
     - If not, the AP is a rogue AP.
   - If OUI and SSID of an AP are configured and both of them are matched, check whether the AP's OUI and SSID are in the authorized OUI and SSID lists.
     - If so, the AP is an authorized AP.
     - If neither or only one of them is in the list, the AP is a rogue AP.
   - If both OUI and SSID of an AP are configured and either of them can be matched, check whether either of AP's OUI and SSID are in the authorized OUI list or SSID list.
     - If both or one of them is in the list, the AP is an authorized AP.
     - If neither of them is in the list, the AP is a rogue AP.

Precautions

If you add or delete an entry, the device will re-check the validity of the rogue APs. If a rogue AP becomes authorized, the device stops containing it. If an authorized AP becomes rogue, the device starts to contain it.

Example

Add an MAC address, an OUI, and an SSID to the WIDS whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-whitelist-profile name default
[HUAWEI-wlan-wids-whitelist-default] permit-ap mac-address 00e0-fc12-3456
```



```
[HUAWEI-wlan-wids-whitelist-default] permit-ap oui 00-11-22
[HUAWEI-wlan-wids-whitelist-default] permit-ap ssid example
```

11.11.50 permit-ap oui-ssid-match

Function

The **permit-ap oui-ssid-match** command configures an OUI and SSID matching policy in a WIDS whitelist.

The **undo permit-ap oui-ssid-match** command deletes the OUI and SSID matching policy in a WIDS whitelist.

By default, both OUIs and SSIDs are matched in a WIDS whitelist.

Format

permit-ap oui-ssid-match { **both** | **any** }

undo permit-ap oui-ssid-match

Parameters

Parameter	Description	Value
both	Matches both OUIs and SSIDs in a WIDS whitelist.	-
any	Matches either of OUIs and SSIDs in a WIDS whitelist.	-

Views

WIDS whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After WIDS or WIPS is enabled, you can run the **permit-ap** command to configure a WIDS whitelist, including the authorized MAC address list, authorized OUI list, and authorized SSID list. If a rogue AP is detected but matches the authorized AP list, the AP is considered an authorized AP and will not be contained.

This command is used to configure a policy for matching OUIs and SSIDs in the WIDS whitelist.

- Both: Both the OUI and SSID of an AP are matched against the authorized OUI list and authorized SSID list. If no match is found in the lists, the AP is considered a rogue AP. If only one of authorized OUI and SSID lists is

configured in the WIDS whitelist, the device matches the OUI or SSID of the AP only against the configured list.

- Any: The OUI and SSID of an AP is matched against the authorized OUI list or the authorized SSID list accordingly. If a match is found in either of the lists, the AP is considered an authorized AP; if not, the AP is considered a rogue AP.

Precautions

After the OUI and SSID matching policy is modified, the device checks whether the AP is authorized. If not, the device determines the containment policy. If a rogue AP becomes authorized, the device stops containing it. If an authorized AP becomes rogue, the device starts to contain it.

Example

Set the OUI and SSID matching policy in a WIDS whitelist to **any**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-whitelist-profile name default
[HUAWEI-wlan-wids-whitelist-default] permit-ap oui 00-11-22
[HUAWEI-wlan-wids-whitelist-default] permit-ap ssid example
[HUAWEI-wlan-wids-whitelist-default] permit-ap oui-ssid-match any
```

11.11.51 pmf

Function

The **pmf** command enables the Protected Management Frame (PMF) function of a VAP.

The **undo pmf** command disables the PMF function for a VAP.

By default, the PMF function is disabled for a VAP.

Format

pmf { **optional** | **mandatory** }

undo pmf

Parameters

Parameter	Description	Value
optional	Indicates the optional mode, in which STAs can access the VAP regardless of whether the STAs support PMF or not, but the VAP encrypts only management frames of PMF-capable STAs.	-

Parameter	Description	Value
mandatory	Indicates the mandatory mode, in which the VAP permits access only from PMF-capable STAs.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PMF is a specification released by Wi-Fi Alliance (WFA) based on IEEE 802.11w standards. It aims to apply security measures defined in WPA2, WPA3, OWE to unicast and multicast management action frames to improve network credibility.

If management frames transmitted on WLANs are not encrypted, the following security problems may be introduced. PMF can address the problems.

- Hackers intercept management frames exchanged between the APs and users.
- Hackers pretend to be APs and send Disassociation and Deauthentication frames to disconnect users.
- Hackers pretend to be users and send Disassociation frames to APs to disconnect the users.

Precautions

The authentication and encryption mode in a security profile must be set to WPA2–AES/WPA2-WPA3/WPA3/OWE.

If the authentication mode is WPA3, this command does not take effect. If the authentication mode is WPA3-SAE or WPA3-802.1X, the PMF mode is fixed at **mandatory**. If the authentication mode is WPA2-WPA3, the PMF mode is fixed at **optional**.

If the authentication mode is OWE or its transition mode, this command does not take effect, and the PMF mode is fixed at **mandatory**.

Modifying configuration in the security profile will disconnect all users on the VAP that uses the security profile. The users need to reassociate with the VAP to go online.

The PMF function cannot be deployed on Mesh networks.

Example

Enable the PMF function in optional mode.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2 psk pass-phrase abcdfffffg aes
[HUAWEI-wlan-sec-prof-p1] pmf optional
```

11.11.52 reset wlan ids attack-detected

Function

The **reset wlan ids attack-detected** command deletes information about the attacking devices detected.

Format

reset wlan ids attack-detected { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes information about all types of attacking devices.	-
flood	Deletes information about devices launching flood attacks.	-
spoof	Deletes information about devices launching spoofing attacks.	-
wapi-psk	Deletes information about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Deletes information about devices launching weak IV attacks.	-
wep-share-key	Deletes information about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Deletes information about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Deletes information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Deletes information about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, information about attacking devices detected is recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-detected** command to delete the information.

Example

Delete information about all the current attacking devices.

```
<HUAWEI> reset wlan ids attack-detected all
```

11.11.53 reset wlan ids attack-detected statistics

Function

The **reset wlan ids attack-detected statistics** command deletes the number of attacks detected.

Format

reset wlan ids attack-detected statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, the number of attacks detected is recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-detected statistics** command to delete the information.

Example

Delete the number of attacks detected.

<HUAWEI> **reset wlan ids attack-detected statistics**

11.11.54 reset wlan ids attack-history

Function

The **reset wlan ids attack-history** command deletes historical records about the attacking devices detected.

Format

reset wlan ids attack-history { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes historical records about all types of attacking devices.	-
flood	Deletes historical records about devices launching flood attacks.	-
spoof	Deletes historical records about devices launching spoofing attacks.	-
wapi-psk	Deletes historical records about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Deletes historical records about devices launching weak IV attacks.	-
wep-share-key	Deletes historical records about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Deletes historical records about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Deletes historical records about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Deletes historical records about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, historical records about attacking devices detected are recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-history** command to delete the information.

Example

Delete historical records about all the current attacking devices.

```
<HUAWEI> reset wlan ids attack-history all
```

11.11.55 reset wlan dynamic-blacklist

Function

The **reset wlan dynamic-blacklist** command deletes information about devices in the dynamic blacklist.

Format

reset wlan dynamic-blacklist { **ap-id** *ap-id* | **ap-name** *ap-name* | **mac-address** *mac-address* | **all** }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Deletes the dynamic blacklist information reported by the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Deletes the dynamic blacklist information reported by the AP with a specified name.	The AP name must exist.
mac-address *mac-address*	Deletes the device with a specified MAC address from the dynamic blacklist.	The MAC address must exist.
all	Deletes all information in the dynamic blacklist.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset wlan dynamic-blacklist** command is applicable to the following scenarios:

- To re-collect the dynamic blacklist information, run the **reset wlan dynamic-blacklist all** command to delete all information in the dynamic blacklist. After that, the AC re-collects the information.
- To remove an authorized device from the dynamic blacklist, run the **reset wlan dynamic-blacklist mac-address** command to remove the MAC address of the device from the dynamic blacklist. After that, information sent from the device is not rejected.

Precautions

Running the **reset wlan dynamic-blacklist** command affects packet receiving of APs. Exercise caution when running this command.

Example

Delete the device with the MAC address 00E0-FC12-3456 from the dynamic blacklist.

```
<HUAWEI> reset wlan dynamic-blacklist mac-address 00e0-fc12-3456
```

11.11.56 reset wlan ids rogue-history

Function

The **reset wlan ids rogue-history** command deletes historical records of rogue devices.

Format

reset wlan ids rogue-history { **all** | **ap** | **bridge** | **client** | **adhoc** | **ssid** [*ssid*] | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes historical records of all rogue devices.	-
ap	Deletes historical records of rogue APs.	-
bridge	Deletes historical records of rogue bridge devices.	-

Parameter	Description	Value
client	Deletes historical records of rogue user terminals.	-
adhoc	Deletes historical records of rogue ad-hoc devices.	-
ssid [*ssid*]	Deletes historical records of devices with specified SSIDs.	The SSID must exist. To specify an SSID starting with a space, include the SSID with double quotation marks (" "). For example, in the SSID **" hello"**, the double quotation marks at the start and end of the SSID occupy two characters. To specify an SSID starting with a double quotation mark ("), enter an escape character (\) before the double quotation mark. For example, in the SSID **\"hello**, the escape character (\) occupies one character.
mac-address *mac-address*	Deletes historical records of devices with specified MAC addresses.	The value must be an existing MAC address.

Views

All views

Default Level

3: Management level

Usage Guidelines

When there are excessive historical records of rogue devices or their historical records are useless, you can run the **reset wlan ids rogue-history** command to delete the historical records.

Example

Delete all detected historical records of the rogue devices.

```
<HUAWEI> reset wlan ids rogue-history all
```

11.11.57 rogue-device log enable

Function

The **rogue-device log enable** command enables the function of recording rogue device information in the log.

The **undo rogue-device log enable** command disables the function of recording rogue device information in the log.

By default, the function of recording rogue device information in the log is disabled.

Format

rogue-device log enable

undo rogue-device log enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a rogue device is detected after this function is enabled, information about the device is recorded in the log.

Example

Enable the function of recording rogue device information in the log.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rogue-device log enable
```


11.11.58 security dot1x

Function

The **security dot1x** command configures 802.1X authentication and encryption for WPA and WPA2.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security { **wpa** | **wpa2** | **wpa-wpa2** } **dot1x** { **aes** | **tkip** | **aes-tkip** }

security wpa-wpa2 dot1x tkip aes

undo security

Parameters

Parameter	Description	Value
wpa	Configures WPA authentication.	-
wpa2	Configures WPA2 authentication.	-
wpa-wpa2	Configures WPA-WPA2 authentication. STAs can be authenticated using WPA or WPA2.	-
aes	Configures AES encryption.	-
tkip	Configures TKIP encryption.	-
aes-tkip	Configures AES-TKIP encryption. After successful authentication, STAs can use the AES or TKIP algorithm for data encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are two types of WPA/WPA2 authentication: WPA/WPA2-PSK authentication (also called WPA/WPA2-Personal) and WPA/WPA2-802.1X authentication (also

called WPA/WPA2-Enterprise). 802.1X authentication is of high security and is applicable to enterprise networks.

To access a WLAN device using WPA or WPA2 802.1X authentication, run the **security dot1x** command. If multiple types of STAs connect to the network and they support different authentication and encryption modes, you can configure hybrid encryption and authentication modes.

The **security wpa-wpa2 dot1x tkip aes** command indicates that WPA and WPA2 use TKIP and AES for data encryption, respectively.

Precautions

TKIP and AES-TKIP are insecure encryption algorithms. For data encryption, AES is recommended.

The following STAs do not support the WPA2 802.1X authentication and cannot access the AP. You must configure other security policies for the STAs.

- Nokia: N8
- HP: Pre 3

The authentication type in the security profile and authentication profile must both be set to 802.1X authentication. You can run the **display wlan config-errors** command to check whether error messages are generated for authentication type mismatch between the security profile and authentication profile.

The system displays the message only when the security profile has been bound to the other profiles.

If 802.1X authentication and TKIP or AES-TKIP encryption for WPA/WPA2 are configured, the access of non-HT STAs fails to be denied.

The offline management VAP does not support 802.1X authentication and encryption modes. Therefore, if the offline management VAP is enabled for a VAP profile, the VAP profile cannot be bound to a security profile with WPA/WPA2 802.1X authentication and encryption configured. If the VAP profile has been bound to a security profile, the authentication and encryption modes of the security profile cannot be changed to WPA/WPA2 802.1X.

Example

Configure WPA (802.1X authentication and TKIP encryption).

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa dot1x tkip
```

Configure WPA2 (802.1X authentication and TKIP encryption).

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2 dot1x tkip
```

Configure WPA-WPA2 (802.1X authentication and TKIP-AES encryption).

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa-wpa2 dot1x aes-tkip
```


11.11.59 security enhanced-open

Function

The **security enhanced-open** command configures Opportunistic Wireless Encryption (OWE) authentication or authentication and encryption in OWE transition mode.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security enhanced-open aes [**transition-ssid** *ssid*]

undo security

Parameters

Parameter	Description	Value
aes	Configures AES encryption.	-
transition-ssid *ssid*	Specifies an SSID to use open authentication in OWE transition mode. • If this parameter is not specified, OWE authentication is used. • If this parameter is specified, the OWE transition mode is used. **NOTE** In OWE transition mode, you need to configure two VAP profiles on the same radio and set their authentication modes to OWE and open, respectively. Ensure that the parameter **transition-ssid** is set the same as the SSID in the VAP profile using the open security policy but different from the SSID in the VAP profile using OWE authentication. The OWE transition mode takes effect only when a VAP profile on the same radio uses the same SSID as **transition-ssid** and the open security policy, and the corresponding VAP is enabled. If such effective conditions are not met, the device uses OWE authentication.	The value is a string of 1 to 32 case-sensitive characters without spaces. If spaces are contained in the SSID, enclose the string using double quotation marks ("). For example, if an SSID is **a bc**, enter **"a bc"** when specifying this parameter. In this case, the string can contain a maximum of 30 characters. If the first character of an SSID is a double quotation mark ("), add a backslash (\) to the SSID as the prefix. For example, if an SSID is **"abc**, enter **\"abc** when specifying this parameter. In this case, the string can contain a maximum of 31 characters.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OWE is a Wi-Fi Enhanced Open authentication mode that allows users to access the network without entering the password. In OWE authentication mode, the device uses the AES encryption algorithm to encrypt data on the network, thereby protecting data exchange between STAs and the Wi-Fi network. The OWE transition mode provides backward compatibility with STAs that do not support OWE authentication. That is, these STAs access the network in open-system authentication mode, while OWE-capable STAs access the network in OWE authentication mode.

Precautions

- OWE authentication or its transition mode automatically enables the PMF function in mandatory mode. That is, the **pmf** { **optional** | **mandatory** } command configuration does not take effect in OWE authentication or its transition mode.
- OWE authentication depends on the PMF function, but 802.11n APs do not support the PMF function. Therefore, 802.11n APs do not support OWE authentication.
- OWE authentication and 802.11r cannot be enabled at the same time.
- OWE authentication is not supported in WDS and Mesh scenarios.
- If the security profile is bound to another profile, running this command may interrupt services.
- Some STAs may fail to access the network in OWE or OWE transition mode due to compatibility issues.
- Some OWE-capable STAs may still access the network through open system authentication in OWE transition mode due to compatibility issues.

Example

Set the authentication mode to the OWE transition mode and the SSID using the open-system authentication mode to **wlan-net**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security enhanced-open aes transition-ssid wlan-net
```

11.11.60 security open

Function

The **security open** command configures open-system authentication.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security open

undo security

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Open-system authentication is applicable to public venues where users move frequently and do not need to be authenticated, such as airports and stations. That is, users can access the network without authentication and encryption.

Precautions

It is not secure to use open system authentication independently. Any wireless terminals can access the network without authentication. You are advised to configure open system authentication together with Portal authentication or MAC address authentication.

Example

Configure open-system authentication.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security open
```

11.11.61 security psk

Function

The **security psk** command configures WPA/WPA2 PSK authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security { **wpa** | **wpa2** | **wpa-wpa2** } **psk** { **pass-phrase** | **hex** } *key-value* { **aes** | **tkip** | **aes-tkip** }

security wpa-wpa2 psk { **pass-phrase** | **hex** } *key-value* **tkip aes**

undo security

Parameters

Parameter	Description	Value
wpa	Configures WPA authentication.	-
wpa2	Configures WPA2 authentication.	-
wpa-wpa2	Configures WPA-WPA2 authentication. STAs can be authenticated using WPA or WPA2.	-
psk	Configures PSK authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number. The password of **hex** does not have enough complexity, so **pass-phrase** is recommended.	-

Parameter	Description	Value
key-value	Specifies a password in cipher text.	The value is of 8 to 63 ASCII characters in plain text, 64 hexadecimal characters in plain text, or 48 or 68 or 88 or 108 characters in cipher text. The question mark (?) is supported, which you can enter by pressing **Ctrl+T**. A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx 202206**, enter **"YsHsjx 202206"**. **NOTE** For security purposes, you are advised to configure a key that contains at least two of the following: digits, lowercase letters, uppercase letters, and special characters.
aes	Configures AES encryption.	-
tkip	Configures TKIP encryption.	-
aes-tkip	Configures AES-TKIP encryption. After successful authentication, STAs can use the AES or TKIP algorithm for data encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are two types of WPA/WPA2 authentication: WPA/WPA2-PSK authentication (also called WPA/WPA2-Personal) and WPA/WPA2 802.1X authentication (also called WPA/WPA2-Enterprise). 802.1X authentication is of high security and is applicable to enterprise networks.

To access a WLAN device using WPA or WPA2 PSK authentication, run the **security psk** command. If multiple types of STAs are available, you can configure the WPA-WPA2 and AES-TKIP security policy for authentication and data encryption.

The **security wpa-wpa2 psk** { **pass-phrase** | **hex** } *key-value* **tkip aes** command indicates that WPA and WPA2 use TKIP and AES for data encryption, respectively.

Precautions

TKIP and AES-TKIP are insecure encryption algorithms. For data encryption, AES is recommended.

If the key is in hexadecimal notation, you can enter hexadecimal characters without entering 0x.

If a security profile is bound to multiple VAP profiles, it will take a few minutes to configure WPA/WPA2 PSK authentication and encryption in the security profile.

The system displays the message only when the security profile has been bound to the other profiles.

If PSK authentication and TKIP or AES-TKIP encryption for WPA/WPA2 is configured, the access of non-HT STAs fails to be denied.

If the password is changed to one starting or ending with a space (for example, **YsHsjx_202206**) on the device, some STAs (such as STAs running Windows 7) may filter out the space when you change the password on the STAs. This will lead to an association failure. Therefore, it is not recommended that a password starting or ending with a space be set on the device. If such a password has been configured on the device, delete the existing WLAN configuration on a STA, reassociate the STA with the SSID, and enter the password. For detailed terminal types, refer to the *Test Report on Terminal Compatibility*.

Example

Configure WPA-PSK authentication and the authentication key.

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



```
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa psk pass-phrase YsHsjx_202206 aes
```

Configure WPA2-PSK authentication and the authentication key.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2 psk pass-phrase YsHsjx_202206 aes
```

Configure WPA-WPA2 hybrid encryption and PSK authentication.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa-wpa2 psk pass-phrase YsHsjx_202206 aes-tkip
```

11.11.62 security wapi

Function

The **security wapi** command configures the WAPI authentication mode.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wapi psk { **pass-phrase** | **hex** } *key-value*

security wapi certificate

undo security

Parameters

Parameter	Description	Value
certificate	Configures WAPI certificate authentication.	-
psk	Configures WAPI pre-shared key authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number. The password of **hex** does not have enough complexity, so **pass-phrase** is recommended.	-

Parameter	Description	Value
key-value	Specifies a password in cipher text.	In pass-phrase mode, the key is a string of 8 to 63 characters in plaintext, or 48 or 68 or 88 or 108 characters in ciphertext. In hex mode, the key is a string of 8 to 32 hexadecimal numbers, in which the length of the string must be an even, or a string of 48 or 68 characters in ciphertext. A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx 202206**, enter **"YsHsjx 202206"**. **NOTE** For security purposes, you are advised to configure a key that contains at least two of the following: digits, lowercase letters, uppercase letters, and special characters.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WAPI supports two authentication modes: certificate authentication and pre-shared key authentication. When pre-shared key authentication is used, a pre-shared key must be configured.

- If WAPI authentication is specified as a security policy in a security profile, you can run the **wapi authentication-method** command to configure the WAPI authentication mode.
- The **wapi authentication-method** command determines the WAPI authentication and key management mode. When certificate authentication and key management are configured, authentication involves identity authentication and key negotiation, and the authentication server and certificate need to be configured. When pre-shared key authentication is configured, a pre-shared key needs to be configured, and STAs also need to know the pre-shared key. In this situation, authentication just involves key negotiation.

Precautions

The system displays the message only when the security profile has been bound to the other profiles.

Example

Set the WAPI authentication mode to pre-shared key authentication and specify the key.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wapi psk pass-phrase YsHsjx_202206
```

11.11.63 security wep

Function

The **security wep** command configures the WEP authentication mode.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wep [**share-key** | **dynamic**]

undo security

Parameters

Parameter	Description	Value
security wep	Sets the WEP authentication mode to open-system and encrypts service packets using WEP.	-
security wep share-key	When the WEP authentication mode is set to shared-key authentication: ● If the parameter is present, WEP uses the configured shared key to authenticate wireless terminals and encrypt service packets. ● If the parameter is not present, WEP only uses the configured shared key to encrypt the service packets. A shared key is configured on the wireless terminals regardless of whether the parameter is present.	-
security wep dynamic	Sets the WEP authentication mode to dynamic WEP.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can select security policies on a WLAN based on the security level. WEP is a security policy used earlier and has security risks. It can be used in open scenarios that do not require high security.

Table 11-248 Comparing authentication modes

Configuration	Link Authentication Mode	Encryption Mode	Advantage	Disadvantage
security open	open	Not encrypted	Wireless devices can connect to a network without authentication.	STA identities are not checked, bringing security risks. Service data is not WEP-encrypted.
security wep	open	Static WEP encryption	Service data is WEP-encrypted.	STA identities are not checked, bringing security risks.
security wep share-key	Shared key authentication	Static WEP encryption	A shared key is used to enhance security. Service data is WEP-encrypted.	• A long key string must be configured on each device and is difficult to expand. • A static key is used, which is easy to decipher.
security wep dynamic	open	Dynamic WEP encryption	Dynamic WEP encryption for service data provides higher security.	802.1X authentication is also required. The configuration is complex.

Precautions

- If the **security wep** [**share-key**] command is executed, you can run the **wep key** command to configure the pre-shared key. Otherwise, the default pre-shared key is used.
- If the **security wep dynamic** command is executed to configure dynamic WEP, you also need to configure 802.1X authentication. Otherwise, dynamic WEP does not take effect.
- Each AP can have at most four key indexes configured. The key indexes used by different VAPs cannot be the same.

- The system displays the message only when the security profile has been bound to the other profiles.
- If WEP authentication is configured, the function of denying access of non-HT STAs fails to take effect.
- Mobile phones do not support dynamic WEP.
- RUs do not support dynamic WEP.
- The WEP encryption algorithm is insecure. WPA2 or WPA3 is recommended in scenarios that have high security requirements.

Example

Create security profile **p1** and set the authentication mode to **share-key**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wep share-key
```

11.11.64 security wpa2-wpa3 psk-sae

Function

The **security wpa2-wpa3 psk-sae** command configures WPA2-WPA3-SAE authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wpa2-wpa3 psk-sae pass-phrase *key-value* **aes**

undo security

Parameters

Parameter	Description	Value
pass-phrase *key-value*	Specifies the password for WPA2-WPA3-SAE authentication.	The value is of 8 to 63 ASCII characters in plain text, 64 hexadecimal characters in plain text, or 48 or 68 or 88 or 108 characters in cipher text. A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx 202206**, enter **"YsHsjx 202206"**. **NOTE** For security purposes, you are advised to configure a key that contains at least two of the following: digits, lowercase letters, uppercase letters, and special characters.
aes	Configures AES encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WPA2 is still widely used. To allow STAs that do not support WPA3 to access the WPA3 network, the device supports the WPA3-Personal transition mode, that is, WPA2-WPA3-SAE authentication.

WPA3-Personal supports hybrid authentication, allowing for only WPA2-WPA3 authentication and AES encryption.

Precautions

- WPA2-WPA3 hybrid authentication automatically enables the PMF function in optional mode. That is, configuring the **pmf** { **optional** | **mandatory** } command does not take effect in WPA2-WPA3 hybrid authentication scenarios.
- If the security profile is bound to another profile, running this command may interrupt services.

Example

Configure WPA2-WPA3-SAE authentication and set the user password to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2-wpa3 psk-sae pass-phrase YsHsjx_202206 aes
```

11.11.65 security wpa2-wpa3 dot1x

Function

The **security wpa2-wpa3 dot1x** command configures WPA2-WPA3-802.1X authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wpa2-wpa3 dot1x aes

undo security

Parameters

Parameter	Description	Value
aes	Configures AES encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WPA2 is still widely used. To allow STAs that do not support WPA3 to access the WPA3 network, the device supports the WPA3-Enterprise transition mode, that is, WPA2-WPA3-802.1X authentication.

WPA3-Enterprise supports hybrid authentication, allowing for only WPA2-WPA3 authentication and AES encryption.

Precautions

- WPA2-WPA3 hybrid authentication automatically enables the PMF function in optional mode. That is, configuring the **pmf** { **optional** | **mandatory** }

command does not take effect in WPA2-WPA3 hybrid authentication scenarios.

- If the security profile is bound to another profile, running this command may interrupt services.

Example

Configure WPA2-WPA3-802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2-wpa3 dot1x aes
```

11.11.66 security wpa3 dot1x

Function

The **security wpa3 dot1x** command configures WPA3-802.1X authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wpa3 dot1x { **gcmp256** | **aes** }

undo security

Parameters

Parameter	Description	Value
gcmp256	Indicates the AES-GCM encryption algorithm using a 256-bit key.	-
aes	Configures AES encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WPA3 authentication is classified into the enterprise edition and personal edition, that is, WPA3-802.1X authentication and WPA3-SAE authentication.

Compared with WPA2-802.1X authentication, WPA3-802.1X authentication enhances the algorithm strength by increasing the key length to 192 bits (WPA2 uses a 128-bit encryption key). WPA3-802.1X authentication is applicable to scenarios with high security requirements, such as governments and large enterprises.

WPA3-802.1X authentication has specific requirements on terminals and servers. To deploy WPA3-802.1X authentication, you may need to upgrade related hardware.

Precautions

- WPA3 authentication automatically enables the PMF function in mandatory mode. That is, configuring the **pmf** { **optional** | **mandatory** } command does not take effect in WPA3 authentication scenarios.
- WPA3-802.1X authentication is supported only by APs in compliance with 802.11ac Wave 2 or higher standards.
- WPA3 and 802.11r cannot be used at the same time.
- WPA3 authentication is not supported in WDS and mesh scenarios.
- If the security profile is bound to another profile, running this command may interrupt services.

Example

Configure the WPA3-802.1X authentication mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa3 dot1x gcmp256
```

11.11.67 security wpa3 sae

Function

The **security wpa3 sae** command configures WPA3-SAE authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wpa3 sae pass-phrase *key-value* **aes**

undo security

Parameters

Parameter	Description	Value
pass-phrase *key-value*	Specifies the password for WPA3-SAE authentication.	The value is of 8 to 63 ASCII characters in plain text, 64 hexadecimal characters in plain text, or 48 or 68 or 88 or 108 characters in cipher text. A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx 202206**, enter **"YsHsjx 202206"**. **NOTE** For security purposes, you are advised to configure a key that contains at least two of the following: digits, lowercase letters, uppercase letters, and special characters.
aes	Configures AES encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WPA3 authentication is classified into the enterprise edition and personal edition, that is, WPA3-802.1X authentication and WPA3-SAE authentication.

Similar to WPA/WPA2-PSK authentication, WPA3-SAE authentication applies to small office networks that do not require high network security or authentication server deployment. However, WPA3-SAE introduces the SAE handshake protocol. Compared with WPA/WPA2-PSK authentication, WPA3-SAE can effectively defend against offline dictionary attacks and increase the difficulty of brute force cracking. In addition, the SAE handshake protocol provides forward secrecy. Even if an attacker knows the password on the network, the attacker cannot decrypt or obtain traffic, greatly improving the security of the WPA3 personal network.

Precautions

- WPA3 authentication automatically enables the PMF function in mandatory mode. That is, configuring the **pmf** { **optional** | **mandatory** } command does not take effect in WPA3 authentication scenarios.
- WPA3-SAE authentication depends on the PMF function, but 802.11n APs do not support the PMF function. Therefore, 802.11n APs do not support WPA3-SAE authentication.
- WPA3-SAE does not support PPSK authentication.
- WPA3 and 802.11r cannot be used at the same time.
- WPA3 authentication is not supported in WDS and mesh scenarios.
- If the security profile is bound to another profile, running this command may interrupt services.

Example

Configure WPA3-SAE authentication and set the user password to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa3 sae pass-phrase YsHsjx_202206 aes
```

11.11.68 security-profile (WLAN view)

Function

The **security-profile** command creates a security profile or enters the security profile view.

The **undo security-profile** command deletes a security profile according to the ID or name.

By default, security profiles **default**, **default-wds** and **default-mesh** are available in the system.

Format

security-profile name *profile-name*

undo security-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a security profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

Parameter	Description	Value
all	Deletes all security profiles. **NOTE** Security profiles **default**, **default-wds** and **default-mesh** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure access security. A security profile must be configured before you specify an authentication mode in the profile. To delete a security profile, run the **undo security-profile** command.

The system configures the new profile, the default value is no authentication and no encryption.

Example

Configure a security profile named **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1]
```

11.11.69 security-profile (VAP profile view)

Function

The **security-profile** command binds a security profile to a VAP profile.

The **undo security-profile** command unbinds a security profile from a VAP profile.

By default, the security profile **default** is bound to a VAP profile.

Format

security-profile *profile-name*

undo security-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a security profile.	The security profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to bind a security profile to a VAP profile. The security profile then applies to all users using this VAP profile.

By default, no security policy is configured in a security profile. A VAP can be created on a radio only after a security policy is configured.

Example

Create VAP profile **ChinaNet** and bind security profile **security-profile1** to the VAP profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name ChinaNet
[HUAWEI-wlan-vap-prof-ChinaNet] security-profile security-profile1
```

11.11.70 spoof-detect quiet-time

Function

The **spoof-detect quiet-time** command sets the quiet time for an AP to report the detected spoofing attacks to the AC.

The **undo spoof-detect quiet-time** command restores the default quiet time for an AP to report the detected spoofing attacks to the AC.

By default, the quiet time is 600 seconds for an AP to report the detected spoofing attacks to the AC.

Format

spoof-detect quiet-time *quiet-time-value*

undo spoof-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report the detected spoofing attacks to the AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repeated alarms are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Example

Set the quiet time to 300 seconds for an AP to report the detected spoofing attacks to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect spoof enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] spoof-detect quiet-time 300
```

11.11.71 spoof-ssid

Function

The **spoof-ssid** command configures a fuzzy matching rule for spoofing SSIDs.

The **undo spoof-ssid** command deletes a fuzzy matching rule for spoofing SSIDs.

By default, no fuzzy matching rule is configured for spoofing SSIDs.

Format

spoof-ssid fuzzy-match regex *regex-value*

undo spoof-ssid { **fuzzy-match regex** *regex-value* | **all** }

Parameters

Parameter	Description	Value
fuzzy-match	Configures a fuzzy matching rule to identify spoofing SSIDs.	-
regex *regex-value*	Specifies the regular expression for an SSID. If an SSID matches the regular expression, the SSID is considered a spoofing SSID.	The value is in text format and can contain 1 to 48 case-sensitive characters. It supports Chinese characters or mixture of Chinese and English characters. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
all	Deletes all fuzzy matching rules.	-

Views

WIDS spoof SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WLAN services are available in public places, such as banks and airports. Users can connect to the WLANs after associating with corresponding SSIDs. If a rogue AP is deployed and provides spoofing SSIDs similar to authorized SSIDs, the users may be misled and connect to the rogue AP, which brings security risks. To address this problem, configure a fuzzy matching rule to identify spoofing SSIDs. The device compares a detected SSID with the matching rule. If the SSID matches the rule, the SSID is considered a spoofing SSID. The AP using the spoofing SSID is a rogue AP. After rogue AP containment is configured, the device contains the rogue AP and disconnects users from the spoofing SSID.

Precautions

To make fuzzy matching rules for spoofing SSIDs take effect, enable device detection and rogue device containment so that the device can take countermeasures against rogue APs.

To contain all SSIDs except those on the local device, set the fuzzy matching rule to * and then run the **contain-mode** command to set the containment mode to **spoof-ssid-ap**.

Example

Configure a fuzzy matching rule using the regular expression **^TES[1l]$** to identify spoofing SSIDs **TEST1** or **TESL** similar to **TEST**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-spoof-profile name default
[HUAWEI-wlan-wids-spoof-default] spoof-ssid fuzzy-match regex ^TES[1l]$
```

11.11.72 sta arp-nd-proxy before-assoc

Function

The **sta arp-nd-proxy before-assoc** command enables an AP to send ARP/ND proxy packets for a STA before the STA is successfully associated.

The **undo sta arp-nd-proxy before-assoc** command disables an AP from sending ARP/ND proxy packets for a STA before the STA is successfully associated.

By default, an AP does not send ARP/ND proxy packets for a STA before the STA is successfully associated.

Format

sta arp-nd-proxy before-assoc

undo sta arp-nd-proxy before-assoc

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an AP is enabled to send ARP/ND proxy packets for a STA before the STA succeeds in authentication or key negotiation, the Layer 2 switch connected to the

AP will learn the MAC address of the STA. If an attack floods thousands of STA MAC addresses, the MAC address table on the switch will be seriously corrupted, bringing security risks. To avoid this issue, you can run the **undo sta arp-nd-proxy before-assoc** command to configure the AP to send ARP/ND proxy packets for a STA after the STA succeeds in authentication or key negotiation.

In scenarios with low security requirements, you can run the **sta arp-nd-proxy before-assoc** command to configure the AP to send ARP/ND proxy packets for a STA before the STA is successfully associated to improve link update efficiency.

Precautions

After the **undo sta arp-nd-proxy before-assoc** command is run on an AP, the AP does not send ARP/ND proxy packets for a STA that goes online in open or WEP mode.

Example

Configure an AP to send ARP/ND proxy packets for a STA before the STA is successfully associated.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] sta arp-nd-proxy before-assoc
```

11.11.73 sta-access-mode

Function

The **sta-access-mode** command binds STA blacklist and STA whitelist profiles to VAP profiles or AP system profiles.

The **undo sta-access-mode** command unbinds STA blacklist and STA whitelist profiles from VAP profiles or AP system profiles.

By default, no STA blacklist and STA whitelist profiles are bound to a VAP profile and an AP system profile.

Format

sta-access-mode { **blacklist** | **whitelist** } *profile-name*

undo sta-access-mode

Parameters

Parameter	Description	Value
blacklist	Specifies a STA blacklist profile.	-
whitelist	Specifies a STA whitelist profile.	-
profile-name	Specifies the names of STA blacklist and whitelist profiles.	The STA blacklist and whitelist profiles must exist.

Views

VAP profile view, AP system profile view

Default Level

2: Configuration level

Usage Guidelines

STA blacklists and whitelists configured by using the **sta-mac** command take effect only after the STA blacklist and whitelist profiles are bound to VAP profiles or AP system profiles using the **sta-access-mode** command.

When STA blacklist and whitelist profiles are bound to different profiles, the effective scope of the STA blacklists and whitelists differs.

- VAP profile: The STA blacklist and whitelist take effect on the corresponding VAP.
- AP system profile: The STA blacklist and whitelist take effect on the corresponding AP.
- VAP profile and AP system profile: A STA cannot go online if it cannot meet any of access requirements.

If a STA blacklist or whitelist profile is bound to a VAP profile or an AP system profile, only one STA blacklist or whitelist profile takes effect in the VAP profile or AP system profile.

Example

Bind the STA blacklist profile **sta-blacklist-profile1** to the VAP profile **vap-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] sta-access-mode blacklist sta-blacklist-profile1
```

11.11.74 sta-blacklist-profile

Function

The **sta-blacklist-profile** command creates a STA blacklist profile or displays the STA blacklist profile view.

The **undo sta-blacklist-profile** command deletes one or more STA blacklist profiles.

By default, no STA blacklist profile is created.

Format

sta-blacklist-profile name *profile-name*

undo sta-blacklist-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a STA blacklist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all STA blacklist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the MAC address of a STA is in the blacklist, the STA cannot go online. If the STA blacklist profile is not referenced or the MAC address of a STA is not in the blacklist, the STA is allowed to go online.

The configured blacklist takes effect only after the STA blacklist profile is bound to a VAP profile or an AP system profile using the **sta-access-mode** command.

If a STA is added to the blacklist, the system automatically disconnects the STA.

Precautions

If STA blacklist profiles are bound to a VAP profile and an AP system profile, a STA cannot go online when the MAC address of the STA is in either of the STA blacklist profile.

Example

Create the STA blacklist profile **sta-blacklist-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-blacklist-profile name sta-blacklist-profile1
[HUAWEI-wlan-blacklist-prof-sta-blacklist-profile1]
```


11.11.75 sta-mac

Function

The **sta-mac** command adds the MAC addresses of a STA to the blacklist or whitelist.

The **undo sta-mac** command deletes a specified STA MAC address or all STA MAC addresses from the blacklist or whitelist.

By default, the MAC address of a STA is not added to the blacklist or whitelist.

Format

sta-mac *mac-address* [**description** *description*]

undo sta-mac { *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address	Adds a MAC address to the blacklist or whitelist.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
description	Adds MAC address description to a blacklist or whitelist.	The value is a string of 1 to 80 case-insensitive characters that can include Chinese or Chinese+English characters. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
all	Deletes all MAC addresses from the blacklist or whitelist.	-

Views

STA blacklist profile view, STA whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

If the blacklist function is enabled, all STAs in the blacklist cannot connect to the WLAN.

If the whitelist function is enabled, only STAs in the whitelist can connect to the WLAN.

If a STA is added to the blacklist, the system automatically disconnects the STA.

STAs that have gone online before a whitelist is configured are not forced to go offline even if they are not on the whitelist.

Example

Add the MAC address 00e0-fc12-3456 of a STA to the blacklist profile **sta-blacklist-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-blacklist-profile name sta-blacklist-profile1
[HUAWEI-wlan-blacklist-prof-sta-blacklist-profile1] sta-mac 00e0-FC12-3456
```

11.11.76 sta-whitelist-profile

Function

The **sta-whitelist-profile** command creates a STA whitelist profile or displays the STA whitelist profile view.

The **undo sta-whitelist-profile** command deletes one or more STA whitelist profiles.

By default, no STA whitelist profile is created.

Format

sta-whitelist-profile name *profile-name*

undo sta-whitelist-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a STA whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

Parameter	Description	Value
all	Deletes all STA whitelist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

The configured whitelist takes effect only after the STA whitelist profile is bound to a VAP profile or an AP system profile using the **sta-access-mode** command.

If the configured whitelist takes effect, only STAs in the whitelist can access the WLAN.

STAs that have gone online before a whitelist is configured are not forced to go offline even if they are not on the whitelist.

Example

Create the STA whitelist profile **sta-whitelist-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-whitelist-profile name sta-whitelist-profile1
[HUAWEI-wlan-whitelist-prof-sta-whitelist-profile1]
```

11.11.77 wapi asu

Function

The **wapi asu** command specifies an IP address for an authentication server unit (ASU) server.

The **undo wapi asu** command deletes the IP address of the ASU server.

By default, no IP address is specified for the ASU server.

Format

wapi asu ip *ip-address*

undo wapi asu ip

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the ASU server.	The value is in dotted decimal notation.

Views

Security profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If WAPI certificate authentication is configured, an AC sends WAPI authentication packets to the ASU server at the specified IP address.

Prerequisites

If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi asu** command to specify an IP address for the ASU server.

Precautions

The **wapi asu** command helps to determine to which ASU server WAPI packets are sent. Users must ensure the correctness of both ASU certificates and ASU servers; otherwise, they may fail in user authentication.

The system displays the message only when the security profile has been bound to the other profiles.

Example

Specify IP address 10.164.10.10 for the ASU server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi asu ip 10.164.10.10
```

11.11.78 wapi bk

Function

The **wapi bk** command sets the interval for updating a BK and the BK lifetime percentage.

The **undo wapi bk** command restores the default interval for updating a BK and the BK lifetime percentage.

By default, the interval for updating a BK is 43200s, and the BK lifetime percentage is 70%.

Format

wapi { **bk-threshold** *bk-threshold* | **bk-update-interval** *bk-update-interval* }

undo wapi { **bk-threshold** | **bk-update-interval** }

Parameters

Parameter	Description	Value
bk-threshold *bk-threshold*	Specifies the BK lifetime percentage.	The value is an integer that ranges from 1 to 100.
bk-update-interval *bk-update-interval*	Specifies the interval for updating a BK.	The value is an integer that ranges from 600 to 604800, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

You can set the intervals for updating a BK to ensure security.

The value obtained by multiplying the interval for updating a BK by the BK lifetime percentage should be greater than or equal to 300 seconds. If the interval for updating a BK is less than 300s, the BK may be updated before negotiation is complete due to low STA performance. In this case, some STAs may be forced offline or cannot go online.

Example

Set the interval for updating a BK to 10000s and the BK lifetime percentage to 80%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi bk-update-interval 10000
Warning: If the product of bk-update-interval and bk-threshold is smaller than 300s, users may be forced offline. Continue? [Y/N]:y
[HUAWEI-wlan-sec-prof-p1] wapi bk-threshold 80
```


11.11.79 wapi cert-retrans-count

Function

The **wapi cert-retrans-count** command sets the number of retransmissions of certificate authentication packets.

The **undo wapi cert-retrans-count** command restores the default number of retransmissions of certificate authentication packets.

By default, the number of retransmissions is 3.

Format

wapi cert-retrans-count *cert-count*

undo wapi cert-retrans-count

Parameters

Parameter	Description	Value
cert-count	Specifies the number of retransmissions of certificate authentication packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

If WAPI authentication is specified as a security policy, run the **wapi cert-retrans-count** command to set the number of retransmissions of certificate authentication packets.

Example

Set the number of retransmissions of certificate authentication packets to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi cert-retrans-count 5
```


11.11.80 wapi import certificate

Function

The **wapi import certificate** command imports the AC certificate file, certificate of the AC certificate issuer, and ASU certificate file.

The **undo wapi certificate** command deletes the imported AC certificate file, certificate of the AC certificate issuer, or ASU certificate file.

By default, the AC certificate file, certificate of the AC certificate issuer, and ASU certificate file are not imported.

Format

wapi import certificate { **ac** | **asu** | **issuer** } **format pkcs12 file-name** *file-name* **password** *password*

wapi import certificate { **ac** | **asu** | **issuer** } **format pem file-name** *file-name*

undo wapi certificate { **ac** | **asu** | **issuer** }

Parameters

Parameter	Description	Value
ac	Specifies the AC certificate.	-
asu	Specifies the ASU certificate.	-
issuer	Specifies the certificate of a specified certificate issuer.	-
format pkcs12	Imports a certificate in P12 format.	-
format pem	Imports a certificate in PEM format.	-
file-name *file-name*	Specifies a certificate file name, which the complete path of a certificate file must be specified.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) and cannot start or end with double quotation marks (" ") or spaces.

Parameter	Description	Value
password *password*	Specifies the key of the P12 certificate.	The password can be in plain text or cipher text. • A plain text password is a string of 1 to 32 characters. • A cipher text password is a string of 48 or 68 characters.

Views

Security profile view

Default Level

3: Management level

Usage Guidelines

- If WAPI certificate authentication is specified as a security policy in a security profile, you can run this command to specify the AC certificate, issuer certificate, and ASU certificate. STAs will fail to be authenticated if you do not run this command. The issuer certificate helps to check whether the AC certificate is modified.
- Before using this command, store the AC certificate and ASU certificate to the storage of the device, and import the certificates and private key using SFTP. Certificates must be X509 V3 certificates and comply with the WAPI standard. Otherwise, certificates cannot be imported.
- After this command is run:
  - When an issuer certificate is configured, the system checks correctness of the AC certificate.
  - If the authentication system uses only two certificates, the issuer certificate and ASU certificate have the same certificate file name and are the same certificate. If the authentication system uses three certificates, the issuer certificate and ASU certificate are different from each other and both must be imported.

NOTE

- The ASU certificate and issuer certificate must be imported.
- Certificates to be imported must be valid and correct.
- If the certificates with the same name but different contents have been imported by other security profiles, delete the earlier certificate first.

Example

Import the AC certificate.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi import certificate ac format pem file-name flash:/local_ac.cer
```

11.11.81 wapi import private-key

Function

The **wapi import private-key** command imports the AC private key file.

The **undo wapi private-key** command deletes the imported AC private key file.

By default, no AC private key file is imported.

Format

wapi import private-key format pkcs12 file-name *file-name* **password** *password*

wapi import private-key format pem file-name *file-name*

undo wapi private-key

Parameters

Parameter	Description	Value
format pkcs12	Imports a private key file in P12 format.	-
format pem	Imports a private key file in PEM format.	-
file-name *file-name*	Specifies the name of a private key file.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) and cannot start or end with double quotation marks (" ") or spaces.

Parameter	Description	Value
password *password*	Specifies the password in the private key file of the P12 format.	The password can be in plain text or cipher text. • A plain text password is a string of 1 to 32 characters. • A cipher text password is a string of 48 or 68 characters.

Views

Security profile view

Default Level

3: Management level

Usage Guidelines

- If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi import private-key** command to specify the private key file for the AC certificate.
- Before using this command, store the AC private key file to the storage medium of the device, and import the private key file using SFTP.
- After this command is used, the system obtains the private key file and establishes the mapping between the certificate and private key.

NOTE

The certificate and private key to be imported must be valid and correct.

Example

Import the AC private key file **ac_key.key**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi import private-key format pem file-name flash:/ac_key.key
```

11.11.82 wapi key-update

Function

The **wapi key-update** command sets the USK and MSK update mode.

The **undo wapi key-update** command restores the default USK and MSK update mode.

By default, USKs and MSKs are updated based on time.

Format

wapi { **usk** | **msk** } **key-update** { **disable** | **time-based** }

undo wapi { **usk** | **msk** } **key-update**

Parameters

Parameter	Description	Value
usk	Indicates USK update.	-
msk	Indicates MSK update.	-
disable	Disables key update.	-
time-based	Indicates time-based update. You can run the **wapi msk** and **wapi usk** commands to respectively set the intervals for updating an MSK and a USK.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- To ensure network security, update keys in a timely manner. There are several key update modes.
- The **wapi key-update** command sets the USK and MSK update mode. If the interval for updating an MSK or a USK is too long, key security cannot be ensured.
- If **disable** is specified, keys will not be updated.

Example

Set the USK update mode to time-based update.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi usk key-update time-based
```


11.11.83 wapi msk

Function

The **wapi msk** command sets the interval for updating an MSK, and number of retransmissions of MSK negotiation packets.

The **undo wapi msk** command restores the default interval for updating an MSK, and number of retransmissions of MSK negotiation packets.

By default, the interval for updating an MSK is 86400s; the number of retransmissions of MSK negotiation packets is 3.

Format

wapi { **msk-update-interval** *msk-interval* | **msk-retrans-count** *msk-count* }

undo wapi { **msk-update-interval** | **msk-retrans-count** }

Parameters

Parameter	Description	Value
msk-update-interval *msk-interval*	Specifies the interval for updating an MSK. When the MSK update mode is set to time-based update using the **wapi key-update** command, the interval for updating an MSK needs to be set.	The value is an integer that ranges from 600 to 604800, in seconds.
msk-retrans-count *msk-count*	Specifies the number of retransmissions of MSK negotiation packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. Both the USK and MSK have a lifetime. The USK or MSK needs to be updated when its lifetime ends.

Example

Set the interval for updating an MSK to 10000s, and number of retransmissions of MSK negotiation packets to 5.

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



```
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi msk key-update time-based
[HUAWEI-wlan-sec-prof-p1] wapi msk-update-interval 10000
[HUAWEI-wlan-sec-prof-p1] wapi msk-retrans-count 5
```

11.11.84 wapi sa-timeout

Function

The **wapi sa-timeout** command sets the security association (SA) timeout period for key encryption.

The **undo wapi sa-timeout** command restores the default SA timeout period for key encryption.

The default SA timeout period for key encryption is 60s.

Format

wapi sa-timeout *sa-time*

undo wapi sa-timeout

Parameters

Parameter	Description	Value
sa-time	Specifies the SA timeout period.	The value is an integer that ranges from 1 to 255, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

You can prolong the WAPI timeout period to increase the authentication success ratio.

Example

Set the SA timeout period to 100s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi sa-timeout 100
```


11.11.85 wapi source interface

Function

The **wapi source interface** command configures a source interface for an AC to communicate with an ASU server.

The **undo wapi source interface** command cancels the source interface for an AC to communicate with an ASU server.

By default, no source interface is configured for an AC to communicate with an ASU server.

Format

wapi source interface { **vlanif** *vlan-id* | **loopback** *loopback-number* }

undo wapi source interface

Parameters

Parameter	Description	Value
vlanif *vlan-id*	Configures a VLANIF interface as the source interface.	The value is an integer that ranges from 1 to 4094.
loopback *loopback-number*	Configures a loopback interface as the source interface.	The value is an integer that ranges from 0 to 1023.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In WLAN applications, to use WAPI authentication and enable socket communication between an AC and an ASU server, the AC needs a WAPI source IP address using which all packets are sent to the ASU server.

Prerequisites

An IP address has been assigned to the specified loopback or VLANIF interface.

Precautions

The IP address of the WAPI source interface on the AC must be on the same network segment as the IP address of the ASU server. If no WAPI source interface

is configured, the IP address of the AC source interface is used as the source IP address for sending WAPI packets to the WAPI server by default.

Example

Configure a VLANIF interface as the source interface for the AC to communicate with the ASU server.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.10.1 24
[HUAWEI-Vlanif100] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi source interface Vlanif 100
```

11.11.86 wapi usk

Function

The **wapi usk** command sets the interval for updating a USK, and number of retransmissions of USK negotiation packets.

The **undo wapi usk** command restores the default interval for updating a USK, and number of retransmissions of USK negotiation packets.

By default, the interval for updating a USK is 86400s; the number of retransmissions of USK negotiation packets is 3.

Format

wapi { **usk-update-interval** *usk-interval* | **usk-retrans-count** *usk-count* }

undo wapi { **usk-update-interval** | **usk-retrans-count** }

Parameters

Parameter	Description	Value
usk-update-interval *usk-interval*	Specifies the interval for updating a USK. When the USK update mode is set to time-based update using the **wapi key-update** command, the interval for updating a USK needs to be set.	The value is an integer that ranges from 600 to 604800, in seconds.
usk-retrans-count *usk-count*	Specifies the number of retransmissions of USK negotiation packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. Both the USK and MSK have a lifetime. The USK or MSK needs to be updated when its lifetime ends.

Example

Set the interval for updating a USK to 10000s, and number of retransmissions of USK negotiation packets to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi usk key-update time-based
[HUAWEI-wlan-sec-prof-p1] wapi usk-update-interval 10000
[HUAWEI-wlan-sec-prof-p1] wapi usk-retrans-count 5
```

11.11.87 weak-iv-detect quiet-time

Function

The **weak-iv-detect quiet-time** command sets the quiet time for an AP to report the detected weak IV attacks to the AC.

The **undo weak-iv-detect quiet-time** command restores the default quiet time for an AP to report the detected weak IV attacks to the AC.

By default, the quiet time is 600 seconds for an AP to report the detected weak IV attacks to the AC.

Format

weak-iv-detect quiet-time *quiet-time-value*

undo weak-iv-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report the detected weak IV attacks to the AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repeated alarms are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Example

Set the quiet time to 300 seconds for an AP to report the detected weak IV attacks to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect weak-iv enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] weak-iv-detect quiet-time 300
```

11.11.88 wep default-key

Function

The **wep default-key** command sets the default key ID for WEP authentication or encryption.

The **undo wep default-key** command restores the default key ID for WEP authentication or encryption.

By default, key 0 is used for WEP authentication or encryption.

Format

wep default-key *key-id*

undo wep default-key

Parameters

Parameter	Description	Value
key-id	Specifies the default key ID.	The key ID must exist.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- A maximum of four WEP keys can be configured, and only one WEP key is used for authentication and encryption. This command specifies which key to use.
- After a key ID is specified, the specified key is used for authentication or encryption.
- Each AP can have at most four key indexes configured. The key indexes used by different VAPs cannot be the same.
- The system displays the message only when the security profile has been bound to the other profiles.

Example

Set the default key ID to 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wep default-key 1
```

11.11.89 wep key

Function

The **wep key** command sets a WEP key.

The **undo wep key** command deletes the specified key.

By default, WEP-40 is used. The default username and password are available in *WLAN 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

wep key *key-id* { **wep-40** | **wep-104** | **wep-128** } { { **pass-phrase** | **hex** } *key-value* | **dot1x** }

undo wep key *key-id*

Parameters

Parameter	Description	Value
key-id	Specifies the key ID.	The value is an integer that ranges from 0 to 3.
wep-40	Configures WEP-40 authentication.	-
wep-104	Configures WEP-104 authentication.	-
wep-128	Configures WEP-128 authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number.	-

Parameter	Description	Value
key-value	Specifies a password in cipher text.	The password can be in plain text or cipher text. ● A plain text password is a string of case-sensitive characters. – If WEP-40 is used, the WEP key is 10 hexadecimal characters or 5 ASCII characters. – If WEP-104 is used, the WEP key is 26 hexadecimal characters or 13 ASCII characters. – If WEP-128 is used, the WEP key is 32 hexadecimal characters or 16 ASCII characters. ● A cipher text password is a string of 48 or 68 characters. A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx**

Parameter	Description	Value
		202206, enter **"YsHsjx 202206"**.
dot1x	Specifies dynamic WEP encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To connect to a WLAN device in WEP shared-key authentication mode or dynamic WEP mode, run the **wep key** command to set a WEP key.

NOTE

If the key is in hexadecimal notation, you can enter hexadecimal characters without entering 0x.

Precautions

The system displays the message only when the security profile has been bound to the other profiles.

Example

Configure a WEP key and its ID.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wep key 1 wep-128 hex 12345678123456781234567812345678
```

11.11.90 wids attack detect

Function

(AP group radio view) The **wids attack detect enable** command enables attack detection on all specified radios in an AP group.

(AP group radio view) The **wids attack detect disable** command disables attack detection on all specified radios in an AP group.

(AP group radio view) The **undo wids attack detect enable** command restores the default attack detection configuration on all specified radios in an AP group.

(AP radio view) The **wids attack detect enable** command enables attack detection on an AP radio.

(AP radio view) The **wids attack detect disable** command disables attack detection on an AP radio.

(AP radio view) The **undo wids attack detect** command cancels the configuration of the attack detection function on an AP radio. The status of this function on the AP radio is then determined by the status of this function in the AP group radio view.

By default, attack detection is disabled on an AP radio; flood attack detection, weak IV attack detection, and spoofing attack detection are disabled on radios in the AP group; and brute force key cracking attack detection is enabled on radios in the AP group.

Format

wids attack detect { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** } { **enable** | **disable** }

undo wids attack detect { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** }

Parameters

Parameter	Description	Value
all	Indicates all attack detection functions.	-
flood	Indicates flood attack detection.	-
weak-iv	Indicates weak IV attack detection.	-
spoof	Indicates spoofing attack detection.	-
wpa-psk	Indicates brute force attack detection in WPA-PSK authentication.	-
wpa2-psk	Indicates brute force attack detection in WPA2-PSK authentication.	-
wapi-psk	Indicates brute force attack detection in WAPI-PSK authentication.	-
wep-share-key	Indicates brute force attack detection in shared key authentication.	-

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor and prevent malicious or unintentional attacks on WLANs in real time, network administrators can enable the following attack detection functions based on actual requirements:

- **flood**: indicates flood attack detection used to detect whether an AP receives a large number of packets of the same type in a short period.
- **weak-iv**: indicates weak IV attack detection used to detect whether weak IV is used for WEP encryption on a WLAN.
- **spoof**: indicates spoofing attack detection used to detect whether a potential attacker pretends to be an AP to broadcast Deauthentication and Disassociation packets.
- **wpa-psk**, **wpa2-psk**, **wapi-psk**, or **wep-share-key**: indicates brute force attack detection. If the WPA-PSK, WPA2-PSK, WAPI-PSK, or WEP-SK security policy is configured on a WLAN, brute force attack detection can be enabled to increase the time required for password cracking and improve password security.

Precautions

- The configuration in the AP radio view has a higher priority than that in the AP group radio view.
- After the attack detection function is enabled using the **wids attack detect enable** command, the detected data is stored only on the local device. To report the data to the iMaster NCE-Campus, run the **collect-item user-data enable** command in the SMI view to enable the device to report intelligent O&M data to the iMaster NCE-Campus.
- If no attack detection function is enabled in the AP radio view, the configuration in the AP group radio view is inherited. If any attack detection function is enabled in the AP radio view, the configuration in the AP group radio view does not take effect and the configuration in the AP radio view is inherited. For example, when all attack detection functions are enabled in the AP group radio view:
  - If no attack detection function is enabled in the AP radio view, the configuration in the AP group radio view takes effect. That is, all attack detection functions are enabled on the AP radio.
  - If spoofing attack detection is enabled in the AP radio view, the configuration in the AP radio view takes effect. That is, only spoofing attack detection is enabled on the AP radio.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Run the **attack-device trap enable** command to enable the alarm function for attack detection.

Example

Enable brute force attack detection in WPA-PSK authentication on radio 0 in AP group **default**.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect wpa-psk enable
```

11.11.91 wids manual-contain

Function

The **wids manual-contain** command manually contains specified devices.

The **undo wids manual-contain** command disables containment of specified devices.

By default, no device is manually contained.

Format

wids manual-contain device-mac *device-mac*

undo wids manual-contain { **all** | **device-mac** *device-mac* }

Parameters

Parameter	Description	Value
device-mac *device-mac*	Specifies the MAC address of a device to be contained.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
all	Contains all devices.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **wids manual-contain** command in the WLAN view to manually contain a specified device in a complicated environment.

Precautions

Wireless bridges are not contained.

Example

Contain the AP with the MAC address 00e0-fc04-0004.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids manual-contain device-mac 00e0-fc04-0004
```

11.11.92 wids contain enable

Function

(AP group radio view) The **wids contain enable** command enables rogue or interference device containment on all specified radios in an AP group.

(AP group radio view) The **undo wids contain enable** command disables rogue or interference device containment on all specified radios in an AP group.

(AP radio view) The **wids contain enable** command enables rogue or interference device containment on an AP radio.

(AP radio view) The **undo wids contain enable** command cancels the configuration of the rogue or interference device containment function on an AP radio. The status of this function on the AP radio is then determined by the status of this function in the AP group radio view.

By default, rogue or interference device containment is disabled on AP radios.

Format

wids contain enable

undo wids contain enable

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Rogue or interference devices pose serious security threats to enterprise networks.

After the containment mode is set against rogue or interference APs, the monitor AP uses the identity of the rogue or interference AP to broadcast deauthentication frames to forcibly disconnect STAs. To prevent the STAs from connecting to the rogue or interference AP again, the monitor AP will periodically and continuously send deauthentication frames.

After the containment mode is set against rogue or interference STAs or ad-hoc devices, the monitor AP uses the MAC address of a rogue or interference device to continuously send unicast deauthentication frames.

Precautions

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

After the **keep-service enable** command is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue or interference device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue or interference device and adds it to the containment list. The containment mechanism will disconnect STAs from the AP. Therefore, service holding upon CAPWAP link disconnection does not take effect in this case.

After command **keep-service enable allow new-access** is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue or interference device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue or interference device and adds it to the containment list. The containment mechanism will disable the AP from allowing access of new STAs. Therefore, the function of enabling an offline AP to allow access of new STAs does not take effect in this case.

Follow-up Procedure

Run the **contain-mode** command to set the rogue or interference device containment mode.

Example

Enable rogue or interference device containment on radio 0 in AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids contain enable
```

11.11.93 wids device detect enable

Function

(AP group radio view) The **wids device detect enable** command enables device detection on all specified radios in an AP group.

(AP group radio view) The **undo wids device detect enable** command disables device detection on all specified radios in an AP group.

(AP radio view) The **wids device detect enable** command enables device detection on an AP radio.

(AP radio view) The **undo wids device detect enable** command cancels the configuration of the device detection function on an AP radio. The status of this function on the AP radio is then determined by the status of this function in the AP group radio view.

By default, device detection is disabled on AP radios.

Format

wids device detect enable

undo wids device detect enable

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the wireless device detection function is enabled, the monitoring AP detects information about wireless devices in its coverage range and reports the information to the AC. The AC determines whether unauthorized devices exist on the WLAN.

Precautions

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

After the **keep-service enable** command is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue or interference device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue or interference device and adds it to the containment list. The containment mechanism will disconnect STAs from the AP. Therefore, service holding upon CAPWAP link disconnection does not take effect in this case.

After command **keep-service enable allow new-access** is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue or interference device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue or interference device and adds it to the containment list. The containment mechanism will disable the AP from allowing access of new STAs. Therefore, the function of enabling an offline AP to allow access of new STAs does not take effect in this case.

After the device detection function is enabled using this command, the detected data is stored only on the local device. To report the data to the iMaster NCE-Campus, run the **collect-item user-data enable** command in the SMI view to enable the device to report intelligent O&M data to the iMaster NCE-Campus.

Example

Enable device detection on radio 0 in AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids device detect enable
```

11.11.94 wids-whitelist-profile (WLAN view)

Function

The **wids-whitelist-profile** command creates a WIDS whitelist profile and enters the WIDS whitelist profile view.

The **undo wids-whitelist-profile** command deletes a WIDS whitelist profile.

By default, the system provides the WIDS whitelist profile **default**.

Format

wids-whitelist-profile name *profile-name*

undo wids-whitelist-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WIDS whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" "). Only the default profile **default** is supported.
all	Deletes all WIDS whitelist profiles.	The default WIDS whitelist profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After WIDS/WIPS is enabled, rogue APs can be detected and countered. However, there may be APs of other vendors or on other networks working in the existing signal coverage areas. If these APs are countered, their services will be affected. To prevent this situation, configure an authorized AP list, including an authorized MAC address list, OUI list, and SSID list. If an unauthorized AP is detected but matches the authorized AP list, the AP is considered an authorized AP and will not be countered. After you create and a WIDS whitelist profile using the **wids-whitelist-profile** command, run the **permit-ap** command to configure an authorized AP list.

Follow-up Procedure

Run the **wids-whitelist-profile (WIDS profile view)** command to bind the WIDS whitelist profile to a WIDS profile so that the WIDS whitelist profile can take effect.

Example

Create the WIDS whitelist profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-whitelist-profile name default
[HUAWEI-wlan-wids-whitelist-default]
```

11.11.95 wids-profile (WLAN view)

Function

The **wids-profile** command creates a WIDS profile and enters the WIDS profile view.

The **undo wids-profile** command deletes a WIDS profile.

By default, the system provides the WIDS profile **default**.

You can run the **display wids-profile** command to view the configuration of the WIDS profile **default**.

Format

wids-profile name *profile-name*

undo wids-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WIDS profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" "). Only the default profile **default** is supported.
all	Deletes all WIDS profiles.	The default WIDS profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the WIDS function on a device to detect and counter rogue devices on a WLAN. The WIDS function also enables the device to detect attacks and add devices launching the attacks to a dynamic blacklist. Packets sent from the blacklisted devices will be rejected to protect authorized users.

After you create and a WIDS profile using the **wids-profile** command, you can configure APs to detect and counter rogue or interference devices, and detect attacks in the profile.

Follow-up Procedure

Run the **wids-profile (AP group view and AP view)** command to bind the WIDS profile to an AP group or AP so that the WIDS profile can take effect.

Example

Create the WIDS profile **office**.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-profile name office
[HUAWEI-wlan-wids-prof-office]
```

11.11.96 wids-spoof-profile (WLAN view)

Function

The **wids-spoof-profile** command creates a WIDS spoof SSID profile and enters the WIDS spoof SSID profile view.

The **undo wids-spoof-profile** command deletes a WIDS spoof SSID profile.

By default, the system has a default WIDS spoof SSID profile **default**.

Format

wids-spoof-profile name *profile-name*

undo wids-spoof-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WIDS spoof SSID profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" "). Only the default profile **default** is supported.
all	Deletes all WIDS spoof SSID profiles.	The default WIDS spoof SSID profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WLAN services are available in public places, such as banks and airports. Users can connect to the WLANs after associating with corresponding SSIDs. If a rogue AP is deployed and provides spoofing SSIDs similar to authorized SSIDs, the users may be misled and connect to the rogue AP, which brings security risks. To address this problem, configure a fuzzy matching rule to identify spoofing SSIDs. After you create and a WIDS spoof SSID profile using the **wids-spoof-profile** command, run the **spoof-ssid** command to configure a fuzzy matching rule to identify spoofing SSIDs.

Follow-up Procedure

Run the **wids-spoof-profile (WIDS profile view)** command to bind the WIDS spoof SSID profile to a WIDS profile to make the WIDS spoof SSID profile take effect.

Example

Create the WIDS spoof SSID profile **office**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-spoof-profile name office
[HUAWEI-wlan-wids-spoof-office]
```

11.11.97 work-mode

Function

(AP group radio view) The **work-mode** command sets the working mode of all specified AP radios in an AP group.

(AP group radio view) The **undo work-mode** command restores the default working mode of all specified AP radios in an AP group.

(AP radio view) The **work-mode** command sets the working mode of a specified radio on an AP in an AP group.

(AP radio view) The **undo work-mode** command restores the working mode of a specified radio on an AP to the working mode configured in the AP group radio view.

By default, AP radios work in normal mode.

Format

work-mode { **monitor** [[**proxy-scan**] **dual-band-scan enable**] | **normal** }

undo work-mode

Parameters

Parameter	Description	Value
monitor	Indicates the monitor mode.	-
dual-band-scan enable	Indicates inter-band scanning.	-
proxy-scan dual-band-scan enable	Indicates proxy scanning.	-
normal	Indicates the normal mode.	-

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP can work in two modes:

- **normal**: indicates the normal mode.
  - If air scan functions (such as WIDS, spectrum analysis, and terminal location) are disabled on a radio, the radio is used to transmit common WLAN services.
  - If air scan functions (such as WIDS, spectrum analysis, and terminal location) are enabled on a radio, the radio transmits common WLAN services and also provides the monitoring function. A transient increase in the WLAN service latency may occur, which does not affect network access. However, if any latency-sensitive service (such as videoconferencing) is running, it is recommended that a separate radio be used for air scan.
- **monitor**: indicates the monitor mode.

  In this mode, the radio can only transmit WLAN services scanned by the air interface but cannot transmit common WLAN services.

Precautions

- The change of the radio working mode can lead to service interruption. Users cannot associate with the AP when its radio works in monitor mode.
- The configuration in the AP radio view has a higher priority than that in the AP group radio view.
- In monitor mode, the working channels and power of AP radios change at any time. In this situation, the working channels and power of the AP radios display as **-**.

- Radio 1 does not support inter-band scanning.
- The switching between the proxy scanning mode and other modes may lead to an AP restart.
- If the inter-band or proxy scanning configuration is delivered to an AP that does not support these two modes, the monitor mode takes effect on the AP.

Example

Set the working mode of radio 0 in AP group **default** to **monitor**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] work-mode monitor
Warning: Modify the work mode may cause business interruption, continue?[y/n]
:y
```

11.11.98 wpa ptk-update enable

Function

The **wpa ptk-update enable** command enables periodic PTK update in WPA or WPA2 authentication and encryption.

The **undo wpa ptk-update enable** command disables periodic PTK update.

By default, periodic PTK update is disabled.

Format

wpa ptk-update enable

undo wpa ptk-update enable

Parameters

None

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In WPA or WPA2 authentication and encryption, a Pairwise Transient Key (PTK) is generated at the key negotiation stage to encrypt unicast radio packets. To ensure secure encryption, enable periodic PTK update so that the AP and STA use a new PTK to encrypt radio packets after a regular interval.

Precautions

When periodic PTK update is implemented, some STAs may encounter service interruptions or go offline due to individual problems.

Follow-up Procedure

Run the **wpa ptk-update ptk-update-interval** command to configure the periodic PTK update interval.

Example

Enable the periodic PTK update function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name example
[HUAWEI-wlan-sec-prof-example] wpa ptk-update enable
```

11.11.99 wpa ptk-update ptk-update-interval

Function

The **wpa ptk-update ptk-update-interval** command configures an interval for updating PTKs in WPA or WPA2 authentication and encryption.

The **undo wpa ptk-update ptk-update-interval** command restores the default PTK update interval.

By default, the interval for updating PTKs is 43200 seconds.

Format

wpa ptk-update ptk-update-interval *ptk-rekey-interval*

undo wpa ptk-update ptk-update-interval

Parameters

Parameter	Description	Value
ptk-rekey-interval	Specifies the PTK update interval.	The value is an integer ranging from 43200 to 86400, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure secure encryption during WPA or WPA2 authentication, enable periodic PTK update. You can run this command to configure the PTK update interval. A smaller interval indicates faster PTK update and more secure data encryption. However, if the PTK update interval is set too small, the STA and AP implement more negotiations, affecting the throughput.

Precautions

The configured periodic PTK update interval takes effect only after you enable the periodic PTK update function using the **wpa ptk-update enable** command.

Example

Set the periodic PTK update interval to 50,000 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name example
[HUAWEI-wlan-sec-prof-example] wpa ptk-update ptk-update-interval 50000
```

11.12 WLAN WDS Configuration Commands

The WDS function is not supported by the following AP models:

- AirEngine series APs
- Central APs (including matching RUs)

11.12.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.12.2 dhcp trust port (WDS profile view)

Function

The **dhcp trust port** command enables a DHCP trusted port in a WDS profile.

The **undo dhcp trust port** command disables a DHCP trusted port in a WDS profile.

By default, a DHCP trusted port is enabled in a WDS profile.

Format

dhcp trust port

undo dhcp trust port

Parameters

None

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

After a DHCP trusted port is enabled in a WDS profile and the WDS profile is applied to an AP, the AP receives the DHCP OFFER, ACK, and NAK packets sent by authorized DHCP servers and forwards the packets to STAs so that the STAs can obtain valid IP addresses and go online.

Example

Enable a DHCP trusted port in the WDS profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] dhcp trust port
```

11.12.3 display references wds-profile

Function

The **display references wds-profile** command displays reference information about a WDS profile.

Format

display references wds-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WDS profile.	The WDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wds-profile** command to check reference information about a WDS profile.

Example

Display reference information about the WDS profile **test**.

```
<HUAWEI> display references wds-profile name test
------------------------------------------------------------------------------
Reference type     Reference name                Reference radio  WLAN ID
------------------------------------------------------------------------------
AP group           group-1                       Radio-0          13
AP group           group-1                       Radio-0          14
------------------------------------------------------------------------------
Total: 2
```

Table 11-249 Description of the **display references wds-profile name** command output

Parameter	Description
Reference type	Type of the profile to which the WDS profile is bound.
Reference name	Name of the profile to which the WDS profile is bound. • Run the **wds-profile radio** command in the AP group view or view of the AP with a specified ID to apply a WDS profile. • Run the **wds-profile (AP group radio view or AP radio view)** command in the AP group radio view or AP radio view to apply a WDS profile.
Reference radio	AP radio to which the WDS profile is applied.
WLAN ID	WLAN ID to which the WDS profile is bound.

11.12.4 display references wds-whitelist-profile

Function

The **display references wds-whitelist-profile** command displays reference information about a WDS whitelist profile.

Format

display references wds-whitelist-profile name *whitelist-name*

Parameters

Parameter	Description	Value
name *whitelist-name*	Displays reference information about a specified WDS whitelist profile.	The WDS whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wds-whitelist-profile** command to check reference information about a specified WDS whitelist profile.

Example

Display reference information about the WDS whitelist profile **test**.

```
<HUAWEI> display references wds-whitelist-profile name test
------------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------------
AP group                    profile-1
AP group                    profile-2
------------------------------------------------------------------------------
Total: 2
```

Table 11-250 Description of the **display references wds-whitelist-profile** command output

Parameter	Description
Reference type	Type of the profile to which the WDS whitelist profile is bound.
Reference name	Name of the profile to which the WDS whitelist profile is bound. Run the **wds-whitelist-profile (AP group radio view or AP radio view)** command in the AP group radio view or AP radio view to apply a WDS whitelist profile.

11.12.5 display wds-profile

Function

The **display wds-profile** command displays reference or configuration information about a WDS profile.

Format

display wds-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all WDS profiles.	-
name *profile-name*	Displays information about a specified WDS profile.	The WDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds-profile** command to view the number of times a WDS profile is referenced or configuration information of a specified WDS profile.

Example

Display reference information about all WDS profiles.

```
<HUAWEI> display wds-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
default                          0
test                             2
--------------------------------------------------------------------------------
Total: 2
```


Table 11-251 Description of the **display wds-profile all** command output

Item	Description
Profile name	WDS profile name. To create a WDS profile, run the **wds-profile** command.
Reference	Number of times a WDS profile is referenced.

Display information about the WDS profile **test**.

```
<HUAWEI> display wds-profile name test
--------------------------------------------------------------------------------
WDS name                  : HUAWEI-WLAN-WDS
WDS work mode               : root
Security profile          : test
DHCP trust port             : enable
ND trust port             : enable
MU-MIMO                   : disable
Tagged vlan               : -
Priority map trust        : DSCP
Priority map mode           : DSCP map 802.11e
                        0-7 map 0
                        8-15 map 1
                        16-23 map 2
                        24-31 map 3
                        32-39 map 4
                        40-47 map 5
                        48-55 map 6
                        56-63 map 7
Beacon 2.4G rate(Mbps)    : 1                                   Beacon 5G rate(Mbps)       :
6
--------------------------------------------------------------------------------
```

Table 11-252 Description of the **display wds-profile name** command output

Item	Description
WDS name	WDS name. To set a WDS name, run the **wds-name** command.
WDS work mode	WDS working mode. To set the WDS working mode, run the **wds-mode** command.
Security profile	Security profile bound to a WDS profile. To bind a security profile to a WDS profile, run the **security-profile (WDS profile view)** command.

Item	Description
DHCP trust port	Whether to enable a DHCP trusted port in a WDS profile. ● enable: A DHCP trusted port is enabled. ● disable: A DHCP trusted port is disabled. To enable a DHCP trusted port in a WDS profile, run the **dhcp trust port (WDS profile view)** command.
ND trust port	Whether to enable an ND trusted port in a WDS profile. ● enable: An ND trusted port is enabled. ● disable: An ND trusted port is disabled. To enable an ND trusted port in a Mesh profile, run the **nd trust port (WDS profile view)** command.
MU-MIMO	Whether the MU-MIMO function is enabled. To configure the parameter, run the **mu-mimo disable** command.
Tagged vlan	VLAN configured in a WDS profile. To configure a VLAN in a WDS profile, run the **vlan tagged (WDS profile view)** command.
Priority map trust	Priority mapping trusted by the WDS air interface. To configure the parameter, run the **priority-map trust (WDS profile view)** command.
Priority map mode	Mapping from DSCP priorities to 802.11e user priorities on the WDS air interface. To configure the parameter, run the **priority-map dscp (WDS profile view)** command.
Beacon 2.4G rate	Transmit rate of 2.4 GHz management frames configured in the WDS profile. To configure the parameter, run the **beacon-2g-rate** command.

Item	Description
Beacon 5G rate	Transmit rate of 5 GHz management frames configured in the WDS profile. To configure the parameter, run the **beacon-5g-rate** command.

11.12.6 display wds-whitelist-profile

Function

The **display wds-whitelist-profile** command displays reference or configuration information about a WDS whitelist profile.

Format

display wds-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all WDS whitelist profiles.	-
name *whitelist-name*	Displays information about a specified WDS whitelist profile.	The WDS whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds-whitelist-profile** command to view the number of times a WDS whitelist profile is referenced or MAC addresses added in a specified WDS whitelist profile.

Example

Display reference information about all WDS whitelist profiles.

```
<HUAWEI> display wds-whitelist-profile all
--------------------------------------------------------------------------------
```



```
Profile name                    Reference
--------------------------------------------------------------------------------
default                          0
test                            2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-253 Description of the **display wds-whitelist-profile all** command output

Item	Description
Profile name	Name of a WDS whitelist profile. To create a WDS whitelist profile, run the **wds-whitelist-profile** command.
Reference	Number of times a WDS whitelist profile is referenced.

Display information about the WDS whitelist profile **test**.

```
<HUAWEI> display wds-whitelist-profile name test
--------------------------------------------------------------------------------
WDS whitelist name: test
WDS whitelist MAC list information:
--------------------------------------------------------------------------------
Index     MAC
--------------------------------------------------------------------------------
0         00e0-fcb1-56a0
--------------------------------------------------------------------------------
Total: 1
```

Table 11-254 Description of the **display wds-whitelist-profile name** command output

Item	Description
Index	WDS whitelist ID in a WDS whitelist profile.
MAC	MAC address on a WDS whitelist. To add a MAC address to a WDS whitelist, run the **peer-ap mac (WDS whitelist profile view)** command.

11.12.7 display wds vap

Function

The **display wds vap** command displays information about a WDS VAP.

Format

display wds vap { **ap-group** *ap-group-name* | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] } [**wds-name** *wds-name*]

display wds vap { **all** | **wds-name** *wds-name* }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays information about all WDS VAPs in a specified AP group.	The AP group must exist.
ap-id *ap-id*	Displays information about WDS VAPs on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about WDS VAPs on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about WDS VAPs of a specified AP radio.	The radio ID must exist.
wds-name *wds-name*	Displays information about WDS VAPs of a specified WDS name.	The WDS name must exist.
all	Displays information about all WDS VAPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds vap** command to display information about a WDS VAP.

Example

Display information about all WDS VAPs.

```
<HUAWEI> display wds vap all
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name       RfID WID        WDS name            BSSID         WDS links
--------------------------------------------------------------------------------
1     AP2           0  14         wds                 00e0-fc12-3456  0
1     AP2           0  13         wds                 00e0-fc12-3457  0
0     AP1           0  14         wds                 00e0-fc12-3467  1
0     AP1           0  13         wds                 00e0-fc12-3468  1
```



```
--------------------------------------------------------------------------------
Total: 4
```

Table 11-255 Description of the **display wds vap** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
WID	WLAN ID of a VAP.
WDS name	WDS name. To set a WDS name, run the **wds-name** command.
BSSID	MAC address of a VAP.
WDS links	Number of WDS links.

11.12.8 display wlan wds link

Function

The **display wlan wds link** command displays information about a WDS link.

Format

display wlan wds link { **all** | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] | **wds-profile** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WDS links.	-
ap-id *ap-id*	Displays information about WDS links on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about WDS links on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about WDS links of a specified AP radio.	The radio ID must exist.
wds-profile *profile-name*	Displays information about WDS links in a specified WDS profile.	The WDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan wds link** command to view information about a WDS link.

Example

Display information about all WDS links.

```
<HUAWEI> display wlan wds link all
Rf   : radio ID             Dis  : coverage distance(100m)
Ch   : channel              Per  : drop percent(%)
TSNR : total SNR(dB)        P-   : peer
WDS  : WDS mode             Re   : retry ratio(%)
RSSI : RSSI(dBm)            MaxR : max RSSI(dBm)
-------------------------------------------------------------------------------------------------
APName  P-APName       Rf Dis   Ch   WDS     P-Status    RSSI  MaxR  Per  Re   TSNR  SNR(Ch0~3:dB)
-------------------------------------------------------------------------------------------------
AP_1                1  3     36   root    -          -77   -40   100  100  0    -/-/-/-
AP_2                1  3     36   root    -          -72   -40   56   99   23   21/19/-/-
-------------------------------------------------------------------------------------------------
Total: 2
```

Table 11-256 Description of the **display wlan wds link** command output

Item	Description
APName	Name of the local AP.
P-APName	Name of the peer AP.
Rf	Radio ID of the local AP.
Dis	Radio coverage distance parameter of the local AP.
Ch	Working channel of a WDS link.
WDS	WDS role of the local AP.
P-Status	Status of the peer AP.
RSSI	RSSI of the peer AP.
MaxR	Maximum RSSI threshold of a WDS link.
Per	Packet error ratio of a WDS link.
Re	Packet retransmission ratio of a WDS link.

Item	Description
TSNR	Total SNR of a WDS link.
SNR(Ch0~3:dB)	SNR of each spatial stream of a WDS link.

11.12.9 nd trust port (WDS profile view)

Function

The **nd trust port** command enables an ND trusted port in a WDS profile.

The **undo nd trust port** command disables an ND trusted port in a WDS profile.

By default, an ND trusted port is enabled in a WDS profile.

Format

nd trust port

undo nd trust port

Parameters

None

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

After an ND trusted port is enabled in a WDS profile and the WDS profile is applied to an AP, the AP receives valid ND protocol packets and forwards the packets to STAs or peer APs so that the STAs can obtain valid IPv6 addresses and go online.

Example

Enable an ND trusted port in the WDS profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] nd trust port
```


11.12.10 peer-ap mac (WDS whitelist profile view)

Function

The **peer-ap mac** command adds MAC addresses of neighboring APs that are allowed to connect to an AP to a WDS whitelist profile.

The **undo peer-ap mac** command deletes the MAC addresses of neighboring APs from a WDS whitelist profile.

By default, no MAC address of a neighboring AP is added to a WDS whitelist profile.

Format

peer-ap mac *mac-address*

undo peer-ap mac *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of a neighboring AP to be added to a WDS whitelist profile.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WDS whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WDS whitelist profile is created, you can run the **peer-ap mac** command to add neighboring APs' MAC addresses to the profile.

If a WDS whitelist profile is bound to a WDS profile, only APs with MAC addresses in the WDS whitelist profile can access the local AP, and other APs are denied access.

Precautions

A maximum of six MAC addresses can be added to a WDS whitelist profile.

Example

Create the WDS whitelist profile **whitelist** and add the MAC address **00e0-fc01-0001** to the whitelist profile. Bind the WDS whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-whitelist-profile name whitelist
[HUAWEI-wlan-wds-whitelist-whitelist] peer-ap mac 00e0-fc01-0001
[HUAWEI-wlan-wds-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] wds-whitelist-profile whitelist
```

11.12.11 priority-map dscp (WDS profile view)

Function

The **priority-map dscp** command configures the mapping from DSCP priorities to 802.11e user priorities on the WDS air interface.

The **undo priority-map dscp** command restores the default mapping from DSCP priorities to 802.11e user priorities on the WDS air interface.

Table 11-257 describes the mapping from DSCP priorities to 802.11e user priorities by default.

Table 11-257 Mapping from DSCP priorities to 802.11e user priorities

DSCP Priority	802.11e User Priority
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Format

priority-map dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot11e** *dot11e-value*

undo priority-map dscp

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
dot11e *dot11e-value*	Specifies the 802.11e user priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

On a WDS network, you can run this command to configure the mapping from DSCP priorities to 802.11e user priorities on the WDS air interface of an AP.

Example

Map DSCP priorities 0-6 to 802.11e user priority 0 on the WDS air interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] priority-map dscp 0 to 6 dot11e 0
```

11.12.12 priority-map trust (WDS profile view)

Function

The **priority-map trust** command configures the priority mapping to be trusted by the WDS air interface.

The **undo priority-map trust** command restores the default priority mapping to be trusted by the WDS air interface.

By default, the WDS air interface trusts the mapping from DSCP priorities to 802.11e user priorities.

Format

priority-map trust { **dot1p** | **dscp** }

undo priority-map trust

Parameters

Parameter	Description	Value
dot1p	Indicates that the WDS air interface trusts the mapping from 802.1p priorities to 802.11e user priorities.	-
dscp	Indicates that the WDS air interface trusts the mapping from DSCP priorities to 802.11e user priorities.	-

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

On a WDS network, when 802.1p or DSCP priorities in data packets need to be mapped to 802.11e user priorities and the packets are transmitted through a WDS link, run this command.

Example

Configure the WDS air interface to trust the mapping from 802.1p priorities to 802.11e user priorities.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] priority-map trust dot1p
```

11.12.13 security-profile (WDS profile view)

Function

The **security-profile** command binds a security profile to a WDS profile.

The **undo security-profile** command restores the default security profile bound to a WDS profile.

By default, the security profile **default-wds** is bound to a WDS profile.

Format

security-profile *profile-name*

undo security-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the security profile bound to a WDS profile.	The security profile must exist.

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before a WDS profile is applied to an AP radio to set up WDS links, the WDS profile must have a security profile bound to ensure WDS link security.

Precautions

After a security profile is bound to a WDS profile, the authentication policy and encryption mode in the security profile cannot be changed, but the authentication key can be changed.

A WDS profile can only have one security profile bound. If you run the command multiple times in the same WDS profile view, the latest configuration overwrites the old one.

Example

Create the security profile **sec** and set the security policy to WPA2+PSK+AES. Create the WDS profile **test** and bind the security profile to the WDS profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name sec
[HUAWEI-wlan-sec-prof-sec] security wpa2 psk pass-phrase YsHsjx_202206 aes
[HUAWEI-wlan-sec-prof-sec] quit
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] security-profile sec
Warning: This action may cause service interruption. Continue?[Y/N]y
```


11.12.14 vlan tagged (WDS profile view)

Function

The **vlan tagged** command adds one or a group of VLANs to a WDS profile in tagged mode.

The **undo vlan tagged** command deletes VLANs from a WDS profile.

By default, no VLAN is configured in a WDS profile.

NOTE

Currently, VLANs can only be added to a WDS profile in tagged mode.

Format

vlan tagged { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan tagged { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the tagged VLAN ID. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters determine a VLAN range. If **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is added to the WDS profile in tagged mode. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	• The value of *vlan-id1* is an integer that ranges from 1 to 4094. • The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes all tagged VLANs from a WDS profile.	-

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Adding VLANs to a WDS profile is equivalent to adding hybrid interfaces to a VLAN. After one or a group of VLANs is added to a WDS profile, the WDS link forwards only the packets with these VLAN IDs from STAs and peer APs.

NOTE

A maximum of 256 VLANs can be added to a WDS profile.

Example

Create the WDS profile **test** and add VLANs 3, 4, 5, 6, 10, and 12 to the WDS profile in **tagged** mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] vlan tagged 3 to 6 10 12
```

11.12.15 wds-mode

Function

The **wds-mode** command sets the WDS mode in a WDS profile.

By default, the WDS mode in a WDS profile is **leaf**.

Format

wds-mode { **root** | **middle** | **leaf** }

Parameters

Parameter	Description	Value
root	Sets the WDS mode to root.	-
middle	Sets the WDS mode to middle.	-
leaf	Sets the WDS mode to leaf.	-

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To connect an AP to an AC through WDS links, use this command to set the WDS mode for an AP radio based on the location of the AP on a WDS network.

In the downlink direction, a root node can connect to a middle or leaf node, and a middle node can connect to a leaf node. A leaf node is the termination node of a WDS link.

Precautions

After changing the WDS mode in a WDS profile, reset the APs using the profile to make the changed WDS mode take effect.

Example

Create the WDS profile **test** and set the WDS mode of the profile to **middle**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] wds-mode middle
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.16 wds-name

Function

The **wds-name** command sets a WDS name for a WDS profile.

The **undo wds-name** command deletes the WDS name of a WDS profile.

By default, the WDS name of a WDS profile is **HUAWEI-WLAN-WDS**.

Format

wds-name *name*

undo wds-name

Parameters

Parameter	Description	Value
name	Specifies the character string that indicates the WDS name.	The value is a string of 1 to 32 case-sensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

A WDS name is similar to an SSID. On a WDS network, an AP radio discovers WDS services provided by other APs based on the WDS name.

Each WDS profile must have a WDS name. The default WDS name of a WDS profile is **HUAWEI-WLAN-WDS**. You can run the **wds-name** command to set a WDS name for a WDS profile.

Example

Create the WDS profile **test** and set the WDS name of the profile to **bridge**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] wds-name bridge
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.17 wds-profile

Function

The **wds-profile** command creates a WDS profile or displays the WDS profile view.

The **undo wds-profile** command deletes a WDS profile.

By default, the system provides the WDS profile **default**.

Format

wds-profile name *profile-name*

undo wds-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WDS profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all WDS profiles. **NOTE** The WDS profile **default** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each WDS profile must have a WDS name. The default WDS name of a WDS profile is **HUAWEI-WLAN-WDS**. You can run the **wds-name** command to set a WDS name for a WDS profile.

Example

Create the WDS profile **test** and set the WDS name of the profile to **bridge**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] wds-name bridge
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.18 wds-profile radio

Function

The **wds-profile radio** command binds a WDS profile to an AP group or AP.

The **undo wds-profile radio** command deletes a WDS profile from an AP group or AP.

By default, no WDS profile is bound to an AP group or AP.

Format

wds-profile *profile-name* **radio** { **all** | *radio-id* }

undo wds-profile radio { **all** | *radio-id* }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the WDS profile bound to an AP or AP group.	The WDS profile must exist.
all	Binds a WDS profile to all AP radios.	-
radio-id	Binds a WDS profile to a specified AP radio.	The radio ID must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WDS profile is bound to an AP or AP group, the AP radio will generate a WDS VAP to provide WDS services. The WDS VAP provides hidden SSIDs for WDS nodes to set up connections.

Prerequisites

A WDS profile has been created and configured properly.

Precautions

Among the VAPs created after a WDS profile is bound to an AP radio, the VAPs with the WLAN IDs 13 and 14 cannot be occupied.

An AP radio can only have one WDS profile bound.

Since the WLAN WDS and Mesh functions are mutually exclusive, the WDS and Mesh profiles cannot be applied to an AP radio at the same time.

Example

Bind the WDS profile **test** to radio **0** of APs in the AP group **group1**.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] wds-profile test radio 0
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.19 wds-profile (AP group radio view or AP radio view)

Function

The **wds-profile** command binds a WDS profile to an AP radio.

The **undo wds-profile** command unbinds a WDS profile from an AP radio.

By default, no WDS profile is bound to an AP radio.

Format

wds-profile *profile-name*

undo wds-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the WDS profile bound to an AP radio.	The WDS profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WDS profile is bound to an AP radio, the radio will generate a WDS VAP to provide WDS services. The WDS VAP provides hidden SSIDs for WDS nodes to set up connections.

Prerequisites

A WDS profile has been created and configured properly.

Precautions

Among the VAPs created after a WDS profile is bound to an AP radio, the VAPs with the WLAN IDs 13 and 14 cannot be occupied.

An AP radio can only have one WDS profile bound.

This command has the same function as the **wds-profile radio** command. You can use either of them.

Example

Bind the WDS profile **test** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] wds-profile test
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.20 wds-whitelist-profile

Function

The **wds-whitelist-profile** command creates a WDS whitelist profile or displays the WDS whitelist profile view.

The **undo wds-whitelist-profile** command deletes a WDS whitelist profile.

By default, no WDS whitelist profile is available in the system.

Format

wds-whitelist-profile name *whitelist-name*

undo wds-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
name *whitelist-name*	Specifies the name of a WDS whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all WDS whitelist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After a WDS whitelist profile is created using the **wds-whitelist-profile** command, you can run the **peer-ap mac (WDS whitelist profile view)** command in the WDS whitelist profile view to add MAC addresses of peer APs that are allowed to set up WDS links with the local AP to the profile.

Example

Create the WDS whitelist profile **whitelist** and add the MAC address **00e0-fc01-0001** to the whitelist profile. Bind the WDS whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-whitelist-profile name whitelist
[HUAWEI-wlan-wds-whitelist-whitelist] peer-ap mac 00e0-fc01-0001
[HUAWEI-wlan-wds-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] wds-whitelist-profile whitelist
```

11.12.21 wds-whitelist-profile (AP group radio view or AP radio view)

Function

The **wds-whitelist-profile** command binds a WDS whitelist profile to an AP radio.

The **undo wds-whitelist-profile** command unbinds a WDS whitelist profile from an AP radio.

By default, no WDS whitelist profile is bound to an AP radio.

Format

wds-whitelist-profile *whitelist-name*

undo wds-whitelist-profile

Parameters

Parameter	Description	Value
whitelist-name	Specifies the name of the WDS whitelist profile bound to an AP radio.	The WDS whitelist profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

After a WDS whitelist profile is applied to an AP radio, the AP radio can only set up WDS links with neighboring APs whose MAC addresses are in the WDS whitelist profile. If no WDS whitelist profile is bound to an AP radio, the AP radio can establish WDS links with any neighboring APs.

NOTE

On a WDS network, a root or middle node controls subnode access by MAC addresses added to the WDS whitelist profile. However, a leaf node does not require a whitelist.

An AP radio can only have one WDS whitelist profile bound. If you run the command multiple times on the same AP radio, the latest configuration overwrites the old one.

Example

Create the WDS whitelist profile **whitelist** and add the MAC address **00e0-fc01-0001** to the whitelist profile. Bind the WDS whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-whitelist-profile name whitelist
[HUAWEI-wlan-wds-whitelist-whitelist] peer-ap mac 00e0-fc01-0001
[HUAWEI-wlan-wds-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] wds-whitelist-profile whitelist
```

11.13 WLAN Mesh Configuration Commands

11.13.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.13.2 dhcp trust port (Mesh profile view)

Function

The **dhcp trust port** command enables a DHCP trusted port in a Mesh profile.

The **undo dhcp trust port** command disables a DHCP trusted port in a Mesh profile.

By default, a DHCP trusted port is enabled in a Mesh profile.

Format

dhcp trust port

undo dhcp trust port

Parameters

None

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

After a DHCP trusted port is enabled in a Mesh profile and the Mesh profile is applied to an AP, the AP receives the DHCP OFFER, ACK, and NAK packets sent by authorized DHCP servers and forwards the packets to STAs so that the STAs can obtain valid IP addresses and go online.

Example

Enable a DHCP trusted port in the Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] dhcp trust port
```

11.13.3 display mesh-profile

Function

The **display mesh-profile** command displays reference or configuration information about Mesh profiles.

Format

display mesh-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all Mesh profiles.	-
name *profile-name*	Displays reference information about a specified Mesh profile.	The Mesh profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mesh-profile** command to view the number of times a Mesh profile is referenced or configuration information of a specified Mesh profile.

Example

Display reference information about all Mesh profiles.

```
<HUAWEI> display mesh-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
default                          0
test                            2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-258 Description of the **display mesh-profile all** command output

Item	Description
Profile name	Mesh profile name. To configure this parameter, run the **mesh-profile** command.
Reference	Number of times a Mesh profile is referenced.

Display information about the Mesh profile **test**.

```
<HUAWEI> display mesh-profile name test
--------------------------------------------------------------------------------
Mesh handover profile           :
Security profile               : default-mesh
Mesh ID                        : HUAWEI-WLAN-MESH
Max link number                 : 32
Link RSSI threshold(dBm)        : -90
Link report interval(s)         : 30
Link aging timeout(s)           : 60
FWA switch                     : enable
FWA EDCA mode                   : manual
DHCP trust port                : enable
ND trust port                  : enable
Tagged VLAN                     : 10
Priority map trust             : DSCP
Priority map mode               : DSCP map 802.11e
                              0-7 map 0
                              8-15 map 1
                              16-23 map 2
                              24-31 map 3
                              32-39 map 4
                              40-47 map 5
                              48-55 map 6
                              56-63 map 7
Client mode                     : disable
```



```
Beacon 2.4G rate(Mbps)          : 1
Beacon 5G rate(Mbps)            : 6
Beacon 6G rate(Mbps)            : 6
--------------------------------------------------------------------------------
Mesh WMM EDCA client parameters:
--------------------------------------------------------------------------------
      ECWmax  ECWmin  AIFSN  TXOPLimit
AC_VO  10      4       7      0
AC_VI  4       3       2      94
AC_BE  10      4       3      0
AC_BK  10      4       7      0
--------------------------------------------------------------------------------
```

Table 11-259 Description of the **display mesh-profile name** command output

Item	Description
Mesh handover profile	Mesh handover profile bound to a Mesh profile. To configure this parameter, run the **mesh-handover-profile (Mesh profile view)** command.
Security profile	Security profile bound to a Mesh profile. To configure this parameter, run the **security-profile (Mesh profile view)** command.
Mesh ID	Mesh ID of a Mesh profile. To configure this parameter, run the **mesh-id** command.
Max link number	Maximum number of Mesh links allowed on an AP. To configure this parameter, run the **max-link-number** command.
Link RSSI threshold	RSSI threshold of a Mesh link. To configure this parameter, run the **link-rssi-threshold** command.
Link report interval	Interval for reporting Mesh link information. To configure this parameter, run the **link-report-interval** command.
Link aging timeout	Aging time of a Mesh link. To configure this parameter, run the **link-aging-time** command.

Item	Description
FWA switch	FWA status in a Mesh profile. • enable: The FWA is enabled. • disable: The FWA is disabled. To configure this parameter, run the **fwa enable** command.
FWA EDCA mode	EDCA mode. • auto: indicates the automatic mode. • manual: indicates the manual mode. To configure this parameter, run the **fwa wmm edca-mode** command.
DHCP trust port	Whether to enable a DHCP trusted port in a Mesh profile. • enable: A DHCP trusted port is enabled. • disable: A DHCP trusted port is disabled. To configure this parameter, run the **dhcp trust port (Mesh profile view)** command.
ND trust port	Whether to enable an ND trusted port in a Mesh profile. • enable: An ND trusted port is enabled. • disable: An ND trusted port is disabled. To configure this parameter, run the **nd trust port (Mesh profile view)** command.
Tagged VLAN	VLAN configured in a Mesh profile. To configure this parameter, run the **vlan tagged (Mesh profile view)** command.
Priority map trust	Priority mapping trusted by the Mesh air interface. To configure this parameter, run the **priority-map trust (Mesh profile view)** command.

Item	Description
Priority map mode	Mapping from DSCP priorities to 802.11e user priorities on the Mesh air interface. To configure this parameter, run the **priority-map dscp (Mesh profile view)** command.
Client mode	Whether to enable the Mesh client mode. • enable: The Mesh client mode is enabled. • disable: The Mesh client mode is disabled.
Beacon 2.4G rate	Transmit rate of 2.4 GHz management frames configured in the Mesh profile. To configure this parameter, run the **beacon-2g-rate** command.
Beacon 5G rate	Transmit rate of 5 GHz management frames configured in the Mesh profile. To configure this parameter, run the **beacon-5g-rate** command.
Beacon 6G rate	Transmit rate of 6 GHz management frames configured in the Mesh profile. To configure this parameter, run the **beacon-6g-rate** command.
AC_VO	AC_VO packets.
AC_VI	AC_VI packets.
AC_BE	AC_BE packets.
AC_BK	AC_BK packets.
ECWmax	Exponent form of the maximum contention window (ECWmax). ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **fwa wmm edca-client** command.
ECWmin	Exponent form of the minimum contention window (ECWmin). ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **fwa wmm edca-client** command.

Item	Description
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure this parameter, run the **fwa wmm edca-client** command.
TXOPLimit	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger TXOPLimit value indicates a longer duration to occupy a channel. To configure this parameter, run the **fwa wmm edca-client** command.

11.13.4 display mesh-whitelist-profile

Function

The **display mesh-whitelist-profile** command displays reference or configuration information about a Mesh whitelist profile.

Format

display mesh-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all Mesh whitelist profiles.	-
name *whitelist-name*	Displays information about a specified Mesh whitelist profile.	The Mesh whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mesh-whitelist-profile** command to view the number of times a Mesh whitelist profile is referenced or MAC addresses added in a specified Mesh whitelist profile.

Example

Display reference information about all Mesh whitelist profiles.

```
<HUAWEI> display mesh-whitelist-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
default                          0
test                            2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-260 Description of the **display mesh-whitelist-profile all** command output

Item	Description
Profile name	Name of a Mesh whitelist profile. To configure this parameter, run the **mesh-whitelist-profile** command.
Reference	Number of times a Mesh whitelist profile is referenced.

Display information about the Mesh whitelist profile **test**.

```
<HUAWEI> display mesh-whitelist-profile name test
--------------------------------------------------------------------------------
Mesh whitelist name: test
Mesh whitelist MAC list information:
--------------------------------------------------------------------------------
Index     MAC
--------------------------------------------------------------------------------
0         00e0-fc76-e360
1         00e0-fc74-9640
--------------------------------------------------------------------------------
Total: 2
```

Table 11-261 Description of the **display mesh-whitelist-profile name** command output

Item	Description
Index	Mesh whitelist ID in a Mesh whitelist profile.

Item	Description
MAC	MAC address on a Mesh whitelist. To configure this parameter, run the **peer-ap mac (Mesh whitelist profile view)** command.

11.13.5 display mesh vap

Function

The **display mesh vap** command displays information about a Mesh VAP.

Format

display mesh vap { **ap-group** *ap-group-name* | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] } [**mesh-id** *mesh-id*]

display mesh vap { **all** | **mesh-id** *mesh-id* }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays information about all Mesh VAPs in a specified AP group.	The AP group must exist.
ap-id *ap-id*	Displays information about Mesh VAPs on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about Mesh VAPs on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about Mesh VAPs of a specified AP radio.	The radio ID must exist.
mesh-id *mesh-id*	Displays information about Mesh VAPs of a specified Mesh ID.	The Mesh ID must exist.
all	Displays information about all Mesh VAPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about a specified Mesh VAP or all Mesh VAPs.

Example

Display information about all Mesh VAPs.

```
<HUAWEI> display mesh vap all
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name       RfID WID  Mesh ID          BSSID          Auth type  Mesh links
--------------------------------------------------------------------------------
1     AP2           0    16   mesh             00E0-FC74-964F WPA2-PSK   0
0     AP1           0    16   mesh             00E0-FC74-964F Open       0
--------------------------------------------------------------------------------
Total: 2
```

Table 11-262 Description of the **display mesh vap** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
WID	WLAN ID of a VAP.
Mesh ID	Mesh ID. To configure this parameter, run the **mesh-id** command.
BSSID	MAC address of a VAP.
Auth type	Authentication type.
Mesh links	Number of Mesh links.

11.13.6 display references mesh-profile

Function

The **display references mesh-profile** command displays reference information about a Mesh profile.

Format

display references mesh-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Mesh profile.	The Mesh profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references mesh-profile** command to check reference information about a Mesh profile.

Example

Display reference information about the Mesh profile **test**.

```
<HUAWEI> display references mesh-profile name test
--------------------------------------------------------------------------------
Reference type     Reference name                Reference radio  WLAN ID
--------------------------------------------------------------------------------
AP group           test1                         Radio-0          16
--------------------------------------------------------------------------------
Total: 1
```

Table 11-263 Description of the **display references mesh-profile** command output

Item	Description
Reference type	Type of the profile to which the Mesh profile is bound.
Reference name	Name of the profile to which the Mesh profile is bound. • Run the **mesh-profile radio** command in the AP group view or view of the AP with a specified ID to apply a Mesh profile. • Run the **mesh-profile (AP group radio view or AP radio view)** command in the AP group radio view to apply a Mesh profile.
Reference radio	AP radio to which a Mesh profile is applied.

Item	Description
WLAN ID	WLAN ID to which a Mesh profile is bound.

11.13.7 display references mesh-whitelist-profile

Function

The **display references mesh-whitelist-profile** command displays reference information about a Mesh whitelist profile.

Format

display references mesh-whitelist-profile name *whitelist-name*

Parameters

Parameter	Description	Value
name *whitelist-name*	Displays reference information about a specified Mesh whitelist profile.	The Mesh whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references mesh-whitelist-profile** command to check reference information about a specified Mesh whitelist profile.

Example

Display reference information about the Mesh whitelist profile **test**.

```
<HUAWEI> display references mesh-whitelist-profile name test
------------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------------
AP group                    default
------------------------------------------------------------------------------
Total: 1
```


Table 11-264 Description of the **display references mesh-whitelist-profile** command output

Item	Description
Reference type	Type of the profile by which a Mesh whitelist profile is referenced.
Reference name	Name of the profile by which a Mesh whitelist profile is referenced. To configure this parameter, run the **mesh-whitelist-profile (AP group radio view or AP radio view)** command in the AP group radio view or AP radio view.

11.13.8 display wlan mesh link

Function

The **display wlan mesh link** command displays information about a Mesh link.

Format

display wlan mesh link { **all** | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] | **mesh-profile** *profile-name* | **peer-mac** *peer-mac* }

Parameters

Parameter	Description	Value
all	Displays information about all Mesh links.	-
ap-id *ap-id*	Displays information about Mesh links on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about Mesh links on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about Mesh links of a specified AP radio.	The radio ID must exist.
mesh-profile *profile-name*	Displays information about Mesh links in a specified Mesh profile.	The Mesh profile must exist.
peer-mac *peer-mac*	Displays information about the Mesh link on a specified peer MAC address.	The MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan mesh link** command to view information about a Mesh link.

Example

Display information about all Mesh links.

```
<HUAWEI> display wlan mesh link all
Rf   : radio ID             Dis  : coverage distance(100m)
Ch   : channel              Per  : drop percent(%)
TSNR : total SNR(dB)        P-   : peer
Mesh : Mesh mode            Re   : retry ratio(%)
RSSI : RSSI(dBm)            MaxR : max RSSI(dBm)
--------------------------------------------------------------------------------------------------------------------------------
----
APName          P-APName        P-APMAC         Rf Dis   Ch      Mesh    P-Status       RSSI  MaxR  Per  Re
TSNR  SNR(dB)
Tx(Mbps)    Rx(Mbps)
--------------------------------------------------------------------------------------------------------------------------------
----
00e0-fcdd-ef80  area_2          00e0-fc04-b500  0  3     6       node    normal         -40   -20   1    17   59
56/55
54          54
area_2          00e0-fcdd-ef80  00e0-fcdd-ef80  0  3     6       portal  normal         -48   -7    0    18   45
34/35/44
54          54
--------------------------------------------------------------------------------------------------------------------------------
----
Total: 2
```

Display information about the Mesh link on a specified peer MAC address.

```
<HUAWEI> display wlan mesh link peer-mac 00e0-fc04-b500
Rf   : radio ID             Dis  : coverage distance(100m)
Ch   : channel              Per  : drop percent(%)
TSNR : total SNR(dB)        P-   : peer
Mesh : Mesh mode            Re   : retry ratio(%)
RSSI : RSSI(dBm)            MaxR : max RSSI(dBm)
--------------------------------------------------------------------------------------------------------------------------------
-----------------
IP Address              : 192.168.200.121
--------------------------------------------------------------------------------------------------------------------------------
-----------------
Link Rf  : 1
Channel utilization      : 45
Channel interference     : 20
--------------------------------------------------------------------------------------------------------------------------------
-------
APName          P-APName        P-APMAC         Rf Dis   Ch      Mesh    P-Status       RSSI  MaxR  Per  Re
TSNR  SNR(dB)
Tx(Mbps)    Rx(Mbps)   LinkStatus
--------------------------------------------------------------------------------------------------------------------------------
-------
00e0-fcdd-ef80  area_2          00e0-fc04-b500  0  3     6       node    normal         -40   -20   1    17   59
56/55
```



```
54          54          active
00e0-fcdd-0000  area_2          00e0-fc04-b500  0  3     6       node    normal          -41   -20   1     17    59
56/55
54          54          inactive
--------------------------------------------------------------------------------------------------------------------
-------
```

Table 11-265 Description of the **display wlan mesh link** command output

Item	Description
APName	Name of the local AP.
P-APMAC	MAC address of the peer AP.
P-APName	Name of the peer AP.
Rf	Radio ID of the local AP.
Dis	Radio coverage distance parameter of the local AP.
Ch	Working channel of a Mesh link.
Mesh	Mesh role of the local AP. • portal: mesh-portal • node: mesh-node • node(leaf): mesh-node (leaf mode)
P-Status	Status of the peer AP.
RSSI	RSSI of the peer AP.
MaxR	Maximum RSSI threshold of a Mesh link.
Per	Packet error ratio of a Mesh link.
Re	Packet retransmission ratio of a Mesh link.
TSNR	Total SNR of Mesh links.
SNR(dB)	SNR of each spatial stream of a Mesh link.
Tx(Mbps)	Transmit rate.
Rx(Mbps)	Receive rate.
LinkStatus	Link status. • active: active in Mesh handover mode • inactive: inactive in Mesh handover mode • -: client mode or a common Mesh network

Item	Description
IP Address	IP address of a vehicle-mounted AP. This item is displayed only when the specified MAC address indicates a vehicle-mounted Fat AP.
Link Rf	Radio used by the vehicle-mounted AP. This item is displayed only when the specified MAC address indicates a vehicle-mounted Fat AP.
Channel utilization	Channel utilization of the vehicle-mounted AP. This item is displayed only when the specified MAC address indicates a vehicle-mounted Fat AP.
Channel interference	Co-channel interference of the vehicle-mounted AP. This item is displayed only when the specified MAC address indicates a vehicle-mounted Fat AP.

11.13.9 display wlan mesh route

Function

The **display wlan mesh route** command displays AP routing information on a Mesh network.

Format

display wlan mesh route { **ap-id** *ap-id* | **ap-name** *ap-name* | **all** }

Parameters

Parameter	Description	Value
ap-id	Displays routing information of the AP with a specified ID on a Mesh network.	The AP ID must exist.
ap-name	Displays routing information of the AP with a specified name on a Mesh network.	The AP name must exist.
all	Displays all APs' routing information on a Mesh network.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view specified or all APs' routing information on a Mesh network, which helps you locate faults on the Mesh network.

Example

Display all APs' routing information on a Mesh network.

```
<HUAWEI> display wlan mesh route all
--------------------------------------------------------------------------------
AP name/MAC/Mesh role/Radio          Next-hop name/MAC/Mesh role/Radio
--------------------------------------------------------------------------------
ap1/00e0-fc74-9640/MP/0              ap2/00e0-fc76-e360/MPP/0
--------------------------------------------------------------------------------
Total: 1
```

Table 11-266 Description of the **display wlan mesh route** command output

Item	Description
AP name	Name of an AP.
MAC	MAC address of the AP.
Mesh role	Role of the AP on the Mesh network.
Radio	Radio ID of the AP.
Next-hop name	Name of the next-hop AP.

11.13.10 fwa wmm edca-client

Function

The **fwa wmm edca-client** command configures EDCA parameters used by the remote AP to negotiate with the AT.

The **undo fwa wmm edca-client** command restores the default EDCA parameters used by the remote AP to negotiate with the AT.

Table 11-267 lists the default EDCA parameter settings.

Table 11-267 Default EDCA parameter settings

Packet Type	Parameters	Description
AC_VO	ECWmax	3
	ECWmin	2
	AIFSN	2
	TXOPLimit	47
AC_VI	ECWmax	4
	ECWmin	3
	AIFSN	2
	TXOPLimit	94
AC_BE	ECWmax	10
	ECWmin	4
	AIFSN	3
	TXOPLimit	0
AC_BK	ECWmax	10
	ECWmin	4
	AIFSN	7
	TXOPLimit	0

Format

fwa wmm edca-client { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo fwa wmm edca-client

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-

Parameter	Description	Value
aifsn *aifsn-value*	Specifies the arbitration inter frame spacing number (AIFSN), which determines the channel idle time.	The value is an integer that ranges from 1 to 15.
ecwmin *ecwmin-value*	Specifies the exponent form of the minimum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be smaller than the *ecwmax-value* value.
ecwmax *ecwmax-value*	Specifies the exponent form of the maximum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than the *ecwmin-value* value.
txoplimit *txoplimit-value*	Specifies the transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger TXOPLimit value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. The unit is 32 microseconds. **NOTE** If the TXOPLimit value is 0, the STA can send only one data frame every time it occupies a channel.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue. These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide differentiated

priorities to the packets and different capabilities to compete for channels. In this way, differentiated services are implemented.

Table 11-268 describes the EDCA parameters.

Table 11-268 EDCA parameter description

Parameter	Meaning
Arbitration Interframe Spacing Number (AIFSN)	The DIFS has a fixed value. WMM provides different DIFS values for different ACs. A large AIFSN value means that the STA must wait for a long time and has a low priority.
Exponent form of CWmin (ECWmin) and exponent form of CWmax (ECWmax)	ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. Together, they determine the average backoff time. Large ECWmin and ECWmax values mean a long average backoff time for the STA and a low STA priority.
Transmission Opportunity Limit (TXOPLimit)	After preempting a channel, the STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value means that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can only send one data frame every time it preempts a channel.

Precautions

- The EDCA parameters configured using the **fwa wmm edca-client** command take effect only after you set the EDCA mode to manual mode using the **fwa wmm edca-mode manual** command.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.

You need to configure EDCA parameters according to actual scenarios. **Table 11-269** shows the configuration of EDCA parameters in voice scenarios, and **Table 11-270** shows the configuration in voice and video hybrid scenarios.

Table 11-269 Recommended configuration of EDCA parameters in voice scenarios

Packet Type	Parameters	Description
AC_VO	ECWmax	4
	ECWmin	2
	AIFSN	2
	TXOPLimit	0

Packet Type	Parameters	Description
AC_VI	ECWmax	5
	ECWmin	3
	AIFSN	5
	TXOPLimit	0
AC_BE	ECWmax	10
	ECWmin	6
	AIFSN	5
	TXOPLimit	0
AC_BK	ECWmax	10
	ECWmin	8
	AIFSN	12
	TXOPLimit	0

Table 11-270 Recommended configuration of EDCA parameters in voice and video hybrid scenarios

Packet Type	Parameters	Description
AC_VO	ECWmax	4
	ECWmin	2
	AIFSN	2
	TXOPLimit	0
AC_VI	ECWmax	5
	ECWmin	3
	AIFSN	5
	TXOPLimit	0
AC_BE	ECWmax	10
	ECWmin	6
	AIFSN	12
	TXOPLimit	0
AC_BK	ECWmax	10
	ECWmin	8

Packet Type	Parameters	Description
	AIFSN	12
	TXOPLimit	0

Example

Configure EDCA parameters of AC_VO packets used by the remote AP to negotiate with the AT.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] fwa wmm edca-mode manual
[HUAWEI-wlan-mesh-prof-test] fwa wmm edca-client ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit
0
```

11.13.11 fwa wmm edca-mode

Function

The **fwa wmm edca-mode** command sets the Enhanced Distributed Channel Access (EDCA) mode.

By default, the automatic EDCA mode is used.

Format

fwa wmm edca-mode { **auto** | **manual** }

Parameters

Parameter	Description	Value
auto	Sets the EDCA mode to automatic. In automatic EDCA mode, ATs automatically adjust EDCA parameters based on the number of ATs connecting to the remote AP.	-

Parameter	Description	Value
manual	Sets the EDCA mode to manual. In manual mode, you can run the **fwa wmm edca-client** command to configure EDCA parameters of the AT. The remote AP negotiates with the AT according to the configured parameters.	-

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios where the AT connects to the remote AP through Mesh links, if the EDCA mode is **auto**, ATs automatically adjust EDCA parameters based on the number of ATs connecting to the remote APif the EDCA mode is **manual**, you can run the **fwa wmm edca-client** command to configure EDCA parameters of the AT. The remote AP then negotiates with the AT according to the configured parameters.

NOTE

- The **fwa wmm edca-mode** command takes effect only after the FWA mode is enabled in the Mesh profile using the **fwa enable** command.
- In automatic EDCA mode, the EDCA parameters manually configured using the **fwa wmm edca-client** command do not take effect on the AP.
- This command applies only to scenarios where the AT connects to the remote AP through Mesh links.

Example

Set the EDCA mode to auto.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] fwa wmm edca-mode auto
```


11.13.12 fwa enable

Function

The **fwa enable** command enables fixed wireless access (FWA) in a Mesh profile.

The **undo fwa enable** command disables FWA in a Mesh profile.

By default, FWA is disabled in a Mesh profile.

FWA is not supported by AirEngine series APs.

Format

fwa enable

undo fwa enable

Parameters

None

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An outdoor Access Terminal (AT) needs to set up a Mesh link with a remote AP to provide network access for downlink STAs connected to the AT. In this case, configure the Mesh service on the remote AP and enable FWA in the Mesh profile so that the AT can connect to the remote AP.

Configuration Impact

The FWA configuration has the following impacts:

- FWA and vehicle-ground fast link handover are mutually exclusive in a Mesh profile.
- The default value of the parameter *link-num* in the **max-link-number** *link-num* command is 32, and the value is in the range of 1 to 32.
- The default RSSI threshold of a Mesh link is fixed at –90 dBm, which cannot be changed using the **link-rssi-threshold** command.
- The Mesh service configuration can be performed without the need to bind a Mesh whitelist profile to the Mesh profile.
- A radio bound to the Mesh profile allows access from only ATs. If ATs are not used, do not enable FWA, which prevents a Mesh service configuration failure.

Example

Enable FWA for the Mesh profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] fwa enable
```

Disable FWA for the Mesh profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] undo fwa enable
```

11.13.13 link-aging-time

Function

The **link-aging-time** command sets the aging time of a Mesh link.

The **undo link-aging-time** command restores the default aging time of a Mesh link.

The default aging time of a Mesh link is 10 seconds.

Format

link-aging-time *aging-time*

undo link-aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of a Mesh link.	The value is an integer that ranges from 5 to 60, in seconds.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

If a Mesh node cannot receive keepalive packets from a neighboring node for a period of time greater than or equal to the aging time of a Mesh link, the Mesh node considers the Mesh link disconnected and will reselect a link.

In a fast changing radio environment, if the aging time of a Mesh link is set to a small value, Mesh links may be frequently disconnected or reselected, causing network flapping. If the aging time of a Mesh link is set to a large value, a Mesh node cannot reselect Mesh links in a timely manner, causing service interruption. Therefore, you need to configure a proper aging time for Mesh links based on actual situations.

Example

Set the aging time of a Mesh link to 10s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] link-aging-time 10
```

11.13.14 link-report-interval

Function

The **link-report-interval** command sets the interval at which an MP reports Mesh link information to the AC.

The **undo link-report-interval** command restores the default interval at which an MP reports Mesh link information to the AC.

By default, an MP reports Mesh link information to the AC at an interval of 30 seconds.

Format

link-report-interval *report-interval*

undo link-report-interval

Parameters

Parameter	Description	Value
report-interval	Specifies the interval at which an MP reports Mesh link information to the AC.	The value is an integer that ranges from 5 to 3600, in seconds. The default value is 30.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network is unstable, an MP may frequently send Mesh link establishment or teardown information to the AC, affecting AC's processing of user services. To solve this problem, run the **link-report-interval** command to configure an MP to periodically send Mesh link information to the AC. After the command is executed, the MP sends link information to the AC only at specified intervals, ensuring normal processing of user services.

Example

Set the interval at which an MP reports Mesh link information to the AC to 20s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] link-report-interval 20
```

11.13.15 link-rssi-threshold

Function

The **link-rssi-threshold** command sets the received signal strength indicator (RSSI) threshold of a mesh link.

The **undo link-rssi-threshold** command restores the default RSSI threshold of a mesh link.

By default, the RSSI threshold of a mesh link is -75 dBm. After the FWA mode is enabled in a Mesh profile, the RSSI threshold of a Mesh link is fixed as -90 dBm.

Format

link-rssi-threshold *threshold-value*

undo link-rssi-threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the RSSI threshold of a mesh link.	The value is an integer that ranges from -90 to -20, in dBm. The default value is -75. After the FWA mode is enabled in a Mesh profile, the RSSI threshold of a Mesh link is fixed as -90 dBm.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RSSI threshold of a mesh link indicates the minimum RSSI of the mesh link. If the RSSI of an MP that joins a WMN is lower than the RSSI threshold configured using the **link-rssi-threshold** command, the routing information table of the mesh link is updated and routing information about the MP is deleted.

The RSSI threshold of a mesh link depends on the distance between two MPs that establish the mesh link. If the two MPs are far from each other, a smaller RSSI threshold is recommended. If the two MPs are close to each other, a larger RSSI threshold is recommended.

Example

Set the RSSI threshold of mesh links to -60 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] link-rssi-threshold -60
```

11.13.16 max-link-number

Function

The **max-link-number** command sets the maximum number of mesh links that can be established between APs.

The **undo max-link-number** command restores the default maximum number of mesh links that can be established between APs.

By default, a maximum of eight mesh links can be established between APs. After you enable FWA for a mesh profile using the **fwa enable** command, a maximum of 32 mesh links can be established between APs by default.

Format

max-link-number *link-num*

undo max-link-number

Parameters

Parameter	Description	Value
link-num	Specifies the maximum number of mesh links that can be established between APs.	The value is an integer that ranges from 1 to 32. **NOTE** After you enable FWA for a mesh profile using the **fwa enable** command, the default value of *link-num* is 32, and the value ranges from 1 to 32.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP sets up too many Mesh links with neighboring APs, network indicators, such as the throughput cannot meet customer needs, affecting user experience. To improve user experience, you can run the **max-link-number** command to set the maximum number of mesh links that can be established between APs according to actual situations.

Impact

If the number of mesh links of an AP has reached the maximum, the AP does not set up new mesh links with neighboring APs.

Example

Set the maximum number of mesh links that can be established between APs to **3**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] max-link-number 3
Warning: This action may cause service interruption. Continue?[Y/N]y
```


11.13.17 mesh-id

Function

The **mesh-id** command sets a Mesh ID for a Mesh profile.

The **undo mesh-id** command restores the Mesh ID of a Mesh profile to the default value.

By default, the Mesh ID of a Mesh profile is **HUAWEI-WLAN-MESH**.

Format

mesh-id *name*

undo mesh-id

Parameters

Parameter	Description	Value
name	Specifies the Mesh ID of a Mesh profile.	The value is a string of 1 to 32 case-sensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

The Mesh ID of a Mesh profile is similar to the SSID. On a Mesh network, AP radios discover available Mesh services of other APs based on the Mesh ID.

Each Mesh profile must have a Mesh ID. The default Mesh ID of a Mesh profile is **HUAWEI-WLAN-MESH**. You can run the **mesh-id** command to set a Mesh ID for a Mesh profile.

Example

Create the Mesh profile **test** and set the Mesh ID of the profile to **mesh-net**.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] mesh-id mesh-net
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.13.18 mesh-profile

Function

The **mesh-profile** command creates a Mesh profile or displays the Mesh profile view.

The **undo mesh-profile** command deletes a Mesh profile.

By default, the system provides the Mesh profile **default**.

Format

mesh-profile name *profile-name*

undo mesh-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Mesh profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all Mesh profiles. **NOTE** The Mesh profile **default** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Mesh profile is applied to an AP radio, Mesh VAPs are created on the radio.

Each Mesh profile must have a Mesh ID. The default Mesh ID of a Mesh profile is **HUAWEI-WLAN-MESH**. You can run the **mesh-id** command to set a Mesh ID for a Mesh profile.

Example

Create the Mesh profile **test** and set the Mesh ID of the profile to **mesh-net**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] mesh-id mesh-net
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.13.19 mesh-profile radio

Function

The **mesh-profile radio** command binds a Mesh profile to an AP group or AP.

The **undo mesh-profile radio** command unbinds a Mesh profile from an AP group or AP.

By default, no Mesh profile is bound to an AP group or AP.

Format

mesh-profile *profile-name* **radio** { **all** | *radio-id* }

undo mesh-profile radio { **all** | *radio-id* }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the Mesh profile bound to an AP group or AP.	The Mesh profile must exist.
all	Binds a Mesh profile to all AP radios.	-
radio-id	Binds a Mesh profile to a specified AP radio.	The radio ID must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Mesh profile is bound to an AP group or AP, a Mesh VAP will be generated on AP radios to provide Mesh services for users.

Prerequisites

A Mesh profile has been created and properly configured.

Precautions

Among the VAPs created after a Mesh profile is bound to a radio, the VAP with the WLAN ID 16 cannot be occupied.

An AP radio can only have one Mesh profile bound.

Since the WLAN WDS and Mesh functions are mutually exclusive, the WDS and Mesh profiles cannot be applied to an AP radio at the same time.

Example

Bind the Mesh profile **test** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] mesh-profile test radio 0
```

11.13.20 mesh-profile (AP group radio view or AP radio view)

Function

The **mesh-profile** command binds a Mesh profile to an AP radio.

The **undo mesh-profile** command unbinds a Mesh profile from an AP radio.

By default, no Mesh profile is bound to an AP radio.

Format

mesh-profile *profile-name*

undo mesh-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the Mesh profile bound to an AP radio.	The Mesh profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Mesh profile is bound to an AP group radio or an AP radio, a Mesh VAP will be generated on the specified AP radio to provide Mesh services for users.

Prerequisites

A Mesh profile has been created and properly configured.

Precautions

Among the VAPs created after a Mesh profile is bound to a radio, the VAP with the WLAN ID 16 cannot be occupied.

An AP radio can only have one Mesh profile bound.

This command has the same function as the **mesh-profile radio** command. You can use either of them.

Example

Bind the Mesh profile **test** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] mesh-profile test
```

11.13.21 mesh-role

Function

The **mesh-role** command configures a Mesh role for an AP in the AP system profile.

The **undo mesh-role** command restores the default Mesh role of an AP in the AP system profile.

By default, the Mesh role of an AP is **mesh-node** not in leaf mode in the AP system profile.

Format

mesh-role { **mesh-portal** | **mesh-node** [**leaf**] }

undo mesh-role

Parameters

Parameter	Description	Value
mesh-portal	Sets the Mesh role of an AP to **mesh-portal** in the AP system profile.	-
mesh-node	Sets the Mesh role of an AP to **mesh-node** in the AP system profile.	-
leaf	Configures a Mesh node to work in leaf mode. If this parameter is not specified, the node works in non-leaf mode.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

APs on a Mesh network can be classified as the following types:

- MP (**mesh-node**): Any Mesh points (MPs) that can support AP functions. They provide both Mesh service and user access service.

  If an MP needs to support low-speed mobility, configure the **mesh-node** AP to work in leaf mode. In leaf mode, the MP functions only as the termination point of a Mesh route and cannot establish a link with an MP that has not gone online and is not enabled with offline service holding.
- MPP (**mesh-portal**): Mesh points that connect the Mesh network to other types of networks and forward communication traffic on a Mesh network.

Configure Mesh roles of APs based on service requirements. If an AP needs to provide both Mesh and user access services, set the Mesh role of the AP to **mesh-node**. If an AP is located at the Mesh network ingress or needs to connect MPs on the local Mesh network to external networks, set the Mesh role of the AP to **mesh-portal**.

NOTE

To ensure the overall Mesh network performance, you are not advised to configure the user access service on a **mesh-portal** AP.

Example

Set the Mesh role of an AP to **mesh-portal** in the AP system profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name test
[HUAWEI-wlan-ap-system-prof-test] mesh-role mesh-portal
```


11.13.22 mesh-route aging-time

Function

The **mesh-route aging-time** command sets the aging time of a Mesh route.

The **undo mesh-route aging-time** command restores the default aging time of a Mesh route.

By default, the aging time of a Mesh route is 5 seconds.

Format

mesh-route aging-time *aging-time*

undo mesh-route aging-time

Parameters

Parameter	Description	Value
aging-time *aging-time*	Specifies the aging time of a Mesh route.	The value is an integer that ranges from 1 to 15, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If a Mesh node cannot receive routing frames from a neighboring node for a period of time greater than or equal to the aging time of a Mesh route, the Mesh node considers the Mesh route unreachable and will reselect a route.

If services are interrupted due to great changes in the radio environment, a smaller value for the aging time of a Mesh route can shorten the service interruption time. However, this may cause frequent route reselection, leading to network flapping. Therefore, you need to configure a proper aging time for Mesh routes based on actual situations.

In Mesh link failover scenarios, you can set the aging time of Mesh routes to 1 second so that Mesh routes can be aged out quickly, achieving fast link failover.

Example

Set the aging time of a Mesh route to 10s.

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



```
[HUAWEI-wlan view] ap-system-profile name test
[HUAWEI-wlan-ap-system-prof-test] mesh-route aging-time 10
```

11.13.23 mesh-whitelist-profile

Function

The **mesh-whitelist-profile** command creates a Mesh whitelist profile or displays the Mesh whitelist profile view.

The **undo mesh-whitelist-profile** command deletes a Mesh whitelist profile.

By default, no Mesh whitelist profile is available in the system.

Format

mesh-whitelist-profile name *whitelist-name*

undo mesh-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
name *whitelist-name*	Specifies the name of a Mesh whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all Mesh whitelist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After a Mesh whitelist profile is created, run the **peer-ap mac (Mesh whitelist profile view)** command in the Mesh whitelist profile view to add MAC addresses of the allowed peer APs to the profile.

Example

Create the Mesh whitelist profile **whitelist** and add the MAC address **0001-0001-0001** to the whitelist profile. Bind the Mesh whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-whitelist-profile name whitelist
[HUAWEI-wlan-mesh-whitelist-whitelist] peer-ap mac 0001-0001-0001
[HUAWEI-wlan-mesh-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] mesh-whitelist-profile whitelist
```

11.13.24 mesh-whitelist-profile (AP group radio view or AP radio view)

Function

The **mesh-whitelist-profile** command binds a Mesh whitelist profile to an AP radio.

The **undo mesh-whitelist-profile** command unbinds a Mesh whitelist profile from an AP radio.

By default, no Mesh whitelist profile is bound to an AP radio.

Format

mesh-whitelist-profile *whitelist-name*

undo mesh-whitelist-profile

Parameters

Parameter	Description	Value
whitelist-name	Specifies the name of the Mesh whitelist profile bound to an AP radio.	The Mesh whitelist profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

After a Mesh whitelist profile is applied to an AP radio, the AP radio can only set up Mesh links with neighboring APs whose MAC addresses are in the Mesh whitelist profile.

NOTE

On a Mesh network where ATs are deployed, after FWA is enabled in a Mesh profile using the **fwa enable** command, you can complete the Mesh service configuration without the need to bind a Mesh whitelist profile to an AP radio. However, in other Mesh application scenarios, an AP radio must have a Mesh whitelist profile bound, and the Mesh whitelist profile must have MAC addresses configured.

An AP radio can only have one Mesh whitelist profile bound. If you run the command multiple times on the same AP radio, the latest configuration overwrites the old one.

Example

Create the Mesh whitelist profile **whitelist** and add the MAC address **0001-0001-0001** to the whitelist profile. Bind the Mesh whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-whitelist-profile name whitelist
[HUAWEI-wlan-mesh-whitelist-whitelist] peer-ap mac 0001-0001-0001
[HUAWEI-wlan-mesh-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] mesh-whitelist-profile whitelist
```

11.13.25 mpp-active-reselection disable

Function

The **mpp-active-reselection disable** command disables active MPP reselection.

The **undo mpp-active-reselection** command enables active MPP reselection.

By default, active MPP reselection is enabled.

Format

mpp-active-reselection disable

undo mpp-active-reselection

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After active MPP reselection is enabled on an MP, the MP evaluates MPPs of the same Mesh ID and on the same channel based on the signal strength of Mesh links, the number of link hops, and the number of Mesh links. If a more preferable MPP is available, the MP selects the MPP as its Mesh gateway.

If active MPP reselection is disabled, an MP can only passively reselect MPPs. When the minimum RSSI of all Mesh links on the optimal route to the current MPP is lower than the RSSI threshold of a Mesh link, the MPP reselection process is triggered.

Precautions

This configuration is invalid for the MPP.

In train-to-ground communication scenarios, this configuration takes effect only on vehicle-mounted APs working in client mode but not those working in Mesh handover mode. This is because in Mesh handover mode, vehicle-mounted APs use the link handover algorithm to select the MPP.

Active MPP reselection will cause service loss. Configure the function according to actual needs.

Example

Disable active MPP reselection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name test
[HUAWEI-wlan-ap-system-prof-test] mpp-active-reselection disable
```

11.13.26 nd trust port (Mesh profile view)

Function

The **nd trust port** command enables an ND trusted port in a Mesh profile.

The **undo nd trust port** command disables an ND trusted port in a Mesh profile.

By default, an ND trusted port is enabled in a Mesh profile.

Format

nd trust port

undo nd trust port

Parameters

None

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

After an ND trusted port is enabled in a Mesh profile and the Mesh profile is applied to an AP, the AP receives valid ND protocol packets and forwards the packets to STAs or peer APs so that the STAs can obtain valid IPv6 addresses and go online.

Example

Enable an ND trusted port in the Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] nd trust port
```

11.13.27 peer-ap mac (Mesh whitelist profile view)

Function

The **peer-ap mac** command adds MAC addresses of neighboring APs that are allowed to connect to an AP to a Mesh whitelist profile.

The **undo peer-ap mac** command deletes the MAC addresses of neighboring APs from a Mesh whitelist profile.

By default, no MAC address of a neighboring AP is added to a Mesh whitelist profile.

Format

peer-ap mac *mac-address*

undo peer-ap mac *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of a neighboring AP to be added to a Mesh whitelist profile.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

Mesh whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Mesh whitelist profile is created, you can run the **peer-ap mac** command to add neighboring APs' MAC addresses to the profile.

If a Mesh whitelist profile is bound to a Mesh profile, only APs with MAC addresses in the Mesh whitelist profile can access the local AP, and other APs are denied access.

Precautions

A maximum of 64 MAC addresses can be added to a Mesh whitelist.

Example

Create the Mesh whitelist profile **whitelist** and add the MAC address **0001-0001-0001** to the whitelist profile. Bind the Mesh whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-whitelist-profile name whitelist
[HUAWEI-wlan-mesh-whitelist-whitelist] peer-ap mac 0001-0001-0001
[HUAWEI-wlan-mesh-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] mesh-whitelist-profile whitelist
```

11.13.28 priority-map dscp (Mesh profile view)

Function

The **priority-map dscp** command configures the mapping from DSCP priorities to 802.11e user priorities on the Mesh air interface.

The **undo priority-map dscp** command restores the default mapping from DSCP priorities to 802.11e user priorities on the Mesh air interface.

Table 11-271 describes the mapping from DSCP priorities to 802.11e user priorities by default.

Table 11-271 Mapping from DSCP priorities to 802.11e user priorities

DSCP Priority	802.11e User Priority
0-7	0
8-15	1
16-23	2
24-31	3

DSCP Priority	802.11e User Priority
32-39	4
40-47	5
48-55	6
56-63	7

Format

priority-map dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot11e** *dot11e-value*

undo priority-map dscp

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
dot11e *dot11e-value*	Specifies the 802.11e user priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

On a Mesh network, you can run this command to configure the mapping from DSCP priorities of 802.3 packets to 802.11e user priorities on the Mesh air interface of an AP.

Example

Map DSCP priorities 0-6 to 802.11e user priority 0 on the Mesh air interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] priority-map dscp 0 to 6 dot11e 0
```

11.13.29 priority-map trust (Mesh profile view)

Function

The **priority-map trust** command configures the priority mapping to be trusted by the Mesh air interface.

The **undo priority-map trust** command restores the default priority mapping to be trusted by the Mesh air interface.

By default, the Mesh air interface trusts the mapping from DSCP priorities to 802.11e user priorities.

Format

priority-map trust { **dot1p** | **dscp** }

undo priority-map trust

Parameters

Parameter	Description	Value
dot1p	Indicates that the Mesh air interface trusts the mapping from 802.1p priorities to 802.11e user priorities.	-
dscp	Indicates that the Mesh air interface trusts the mapping from DSCP priorities to 802.11e user priorities.	-

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

On a Mesh network, when 802.1p or DSCP priorities in data packets need to be mapped to 802.11e user priorities and the packets are transmitted through a Mesh link, run this command.

Example

Configure the Mesh air interface to trust the mapping from 802.1p priorities to 802.11e user priorities.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] priority-map trust dot1p
```

11.13.30 security-profile (Mesh profile view)

Function

The **security-profile** command binds a security profile to a Mesh profile.

The **undo security-profile** command restores the default security profile bound to a Mesh profile.

By default, the security profile **default-mesh** is bound to a Mesh profile.

Format

security-profile *profile-name*

undo security-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the security profile bound to a Mesh profile.	The security profile must exist.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before a Mesh profile is applied to an AP radio to establish Mesh links, the Mesh profile must have a security profile bound to ensure Mesh link security.

Precautions

After a security profile is bound to a Mesh profile, the authentication policy and encryption mode in the security profile cannot be changed, but the authentication key can be changed.

A Mesh profile can only have one security profile bound. If you run the command multiple times in the same Mesh profile view, the latest configuration overwrites the old one.

Example

Create the security profile **sec** and set the security policy to WPA2+PSK+AES. Create the Mesh profile **test** and bind the security profile to the Mesh profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name sec
[HUAWEI-wlan-sec-prof-sec] security wpa2 psk pass-phrase YsHsjx_202206 aes
[HUAWEI-wlan-sec-prof-sec] quit
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] security-profile sec
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.13.31 vlan tagged (Mesh profile view)

Function

The **vlan tagged** command adds one or a group of VLANs to a Mesh profile in tagged mode.

The **undo vlan tagged** command deletes VLANs from a Mesh profile.

By default, no VLAN is configured in a Mesh profile.

Format

vlan tagged { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan tagged { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the tagged VLAN ID. • *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, only the VLAN specified by *vlan-id1* is added to the Mesh profile in tagged mode. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	• The value of *vlan-id1* is an integer that ranges from 1 to 4094. • The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes all tagged VLANs from a Mesh profile.	-

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Mesh network, different VAPs may be configured on the MPP and MPs, or VLANs may be dynamically authorized to STAs on the MPs. If the VLAN or VLANs used by an MP are not created on the MPP, STA packets are discarded on the MPP. To address this, you can run the **vlan tagged** command to create VLANs used by the MPs on the MPP to ensure normal forwarding of STA packets.

Precautions

The VLAN or VLANs specified using the **vlan tagged** command take effect only on the MPP.

A maximum of 256 VLANs can be added to a Mesh profile.

Example

Create the Mesh profile **test** and add VLANs 3, 4, 5, 6, 10, and 12 to the Mesh profile in tagged mode.

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



```
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] vlan tagged 3 to 6 10 12
```

11.13.32 wideband enable

Function

The **wideband enable** command enables the wideband function, that is, the 4.9 GHz frequency band, of the regulatory domain profile.

The **undo wideband enable** command disables the wideband function, that is, the 4.9 GHz frequency band, of the regulatory domain profile.

By default, the wideband function of the regulatory domain profile is disabled.

The 4.9 GHz frequency band is not supported by AirEngine series APs.

NOTE

Before using the 4.9 GHz frequency band, ensure that you have obtained the 4.9 GHz license from the local administrative department and use the band properly.

Format

wideband enable

undo wideband enable

Parameters

None

Views

Regulatory domain profile

Default Level

2: Configuration level

Usage Guidelines

The wideband function enables AP radios on the 5 GHz frequency band to use the 4.9 GHz frequency band. The 4.9 GHz frequency band is applicable only to outdoor backhaul scenarios but not wireless coverage services. It is mainly used by WDS and Mesh backhaul links. The 4.9 GHz frequency band is not within the DFS reselection channel range.

The following table lists channels and frequency distribution of the 4.9 GHz frequency band.

Channel ID	Parameter	Description
184	Frequency band	4.9 GHz

Channel ID	Parameter	Description
	Center frequency (MHz)	4920
	Upper frequency (MHz)	4910
	Lower frequency (MHz)	4930
188	Frequency band	4.9 GHz
	Center frequency (MHz)	4940
	Upper frequency (MHz)	4930
	Lower frequency (MHz)	4950
192	Frequency band	4.9 GHz
	Center frequency (MHz)	4960
	Upper frequency (MHz)	4950
	Lower frequency (MHz)	4970
196	Frequency band	4.9 GHz
	Center frequency (MHz)	4980
	Upper frequency (MHz)	4970
	Lower frequency (MHz)	4990

The 4.9 GHz frequency band supports channel bandwidths of 20 MHz and 40 MHz. Channels 184+188 or 192+196 can be bundled into a 40 MHz channel. Similar to the 5 GHz frequency band, the 4.9 GHz frequency band complies with 802.11a/n/ac.

After the wideband function of the regulatory domain profile is enabled, APs bound to this profile are automatically reset.

Example

Enable the wideband function of the regulatory domain profile.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name test
[HUAWEI-wlan-regulate-domain-test] wideband enable
Warning: To use the 4.9 GHz frequency band, apply for a license from the related department. When this frequency band takes effect,
the AP will be reset. Continue? [Y/N]y
```

11.14 Vehicle-Ground Fast Link Handover Configuration Commands

11.14.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.14.2 antenna-output

Function

The **antenna-output** command configures an output mode of a 2.4G/5G antenna.

The **undo antenna-output** command restores the default output mode of a 2.4G/5G antenna.

By default, a 2.4G/5G antenna uses split output.

Format

antenna-output { **split** | **combine** }

undo antenna-output

Parameters

Parameter	Description	Value
split	Indicates the split mode of a 2.4G/5G antenna.	-
combine	Indicates the combination mode of a 2.4G/5G antenna.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In train-ground communication scenarios, you can use the **antenna-output split** command to configure the split mode of a 2.4G/5G antenna. The antenna uses either the 2.4 GHz radio to provide wireless coverage in the carriage, or the 5 GHz radio to provide wireless bridging between carriages.

In train-ground communication scenarios, you can use the **antenna-output combine** command to configure the combination mode of a 2.4G/5G antenna. The antenna uses the 2.4 GHz and 5 GHz radios to simultaneously provide wireless bridging between carriages.

Precautions

This command is supported only by APs supporting antenna combination and split modes.

Example

Configure the combination mode of a 2.4G/5G antenna.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] antenna-output combine
```

11.14.3 client-mode enable

Function

The **client-mode enable** command enables the Mesh client mode.

The **undo client-mode enable** command disables the Mesh client mode.

By default, the Mesh client mode is disabled.

Format

client-mode enable

undo client-mode enable

Parameters

None

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the Mesh client is enabled for vehicle-mounted APs, trackside APs must also have the Mesh client enabled to set up a Mesh link.

Precautions

The Mesh handover mode and Mesh client mode are mutually exclusive in a Mesh profile.

A vehicle-ground communication scenario supports either the Mesh handover mode or the Mesh client mode, but not both. Ensure that the same Mesh mode (handover or client) is configured on vehicle-mounted APs and trackside APs. Otherwise, Mesh links may fail to be set up for vehicle-ground communication, or services are affected even if Mesh links can be set up.

Radios of a trackside AP cannot have both the Mesh handover and client modes configured. For example, if radio 1 and radio 2 of a trackside AP have the Mesh handover mode and Mesh client mode configured, respectively, the AP will fail to set up a Mesh link with a vehicle-mounted AP.

Example

Enable the Mesh client mode for Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] client-mode enable
```

11.14.4 display mesh-handover-profile

Function

The **display mesh-handover-profile** command displays reference or configuration information about a Mesh handover profile.

Format

display mesh-handover-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all Mesh handover profiles.	-
name *profile-name*	Displays information about a specified Mesh handover profile.	The Mesh handover profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mesh-handover-profile** command to view the number of times a Mesh handover profile is referenced by a Mesh profile or parameter settings of a specified Mesh handover profile.

Example

Display reference information about all Mesh handover profiles.

```
<HUAWEI> display mesh-handover-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
default                          0
test                            2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-272 Description of the **display mesh-handover-profile all** command output

Item	Description
Profile name	Name of a Mesh handover profile. To configure this parameter, run the **mesh-handover-profile** command.
Reference	Number of times a Mesh handover profile is referenced by a Mesh profile.

Display information about the Mesh handover profile **test**.

```
<HUAWEI> display mesh-handover-profile name test
--------------------------------------------------------------------------------
Handover location based algorithm switch        : disable
Handover probe interval(ms)                     : 100
Doppler optimize switch                         : enable
Doppler optimize level                          : low
Hal half-band switch                            : enable
--------------------------------------------------------------------------------
```


Table 11-273 Description of the **display mesh-handover-profile name** command output

Item	Description
Handover location based algorithm switch	Status of the location-based enhanced fast link handover algorithm. • disable: The algorithm is disabled. • enable: The algorithm is enabled. To configure this parameter, run the **location-based-algorithm enable** command.
Handover probe interval	Mesh link probe interval. To configure this parameter, run the **link-probe-interval** command.
Doppler optimize switch	Whether Doppler optimization is enabled in a Mesh handover scenario. • disable: This function is disabled. • enable: This function is enabled. To configure this parameter, run the **doppler-optimize disable** command.
Doppler optimize level	Doppler optimization mode in a Mesh handover scenario. To configure this parameter, run the **doppler-optimize level** command.
Hal half-band switch	Whether the half-band function is enabled on AP radios in Mesh handover scenarios. • disable: This function is disabled. • enable: This function is enabled. To configure this parameter, run the **hal half-band disable** command.

11.14.5 display mesh-neighbor-rssi

Function

The **display mesh-neighbor-rssi** command displays RSSI information collected by an AP.

Format

display mesh-neighbor-rssi [**ap-name** *ap-name* **radio** *radio-id* | **ap-id** *ap-id* **radio** *radio-id*] [**max-neighbor-number** *max-number*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays RSSI information collected by the AP with a specified name. If this parameter is not specified, RSSI information collected by all APs is displayed.	The AP name must exist.
ap-id *ap-id*	Displays RSSI information collected by the AP with a specified ID. If this parameter is not specified, RSSI information collected by all APs is displayed.	The AP ID must exist.
radio *radio-id*	Displays RSSI information collected by a specified radio.	The radio ID must exist.
max-neighbor-number *max-number*	Specifies the maximum number of neighboring APs of which RSSI information collected by the AP can be displayed. If this parameter is not specified, RSSI information about all neighboring APs collected by the AP is displayed.	The value is an integer that ranges from 1 to 256.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command applies only to APs on a Mesh network. A local AP can collect RSSI information of a neighboring AP only when the neighboring AP and local AP are added to Mesh whitelists of each other.

Example

Display RSSI information collected by all APs.

```
<HUAWEI> display mesh-neighbor-rssi
Info: This operation may take a few seconds, please wait.done.
AP name/MAC/Radio/Location-ID  Neighbor AP/MAC/Location-ID  RSSI  Update Time
--------------------------------------------------------------------------------
area_1/00e0-fc12-3456/0/1      -/00e0-fc12-3457/-           -43   20:55:16
--------------------------------------------------------------------------------
Total: 1
```

Table 11-274 Description of the **display mesh-neighbor-rssi** command output

Item	Description
AP name/MAC/Radio/Location-ID	Name, MAC address, radio ID, and location ID of the local AP. **NOTE** If APs are named based on their locations, this field displays as AP name/MAC/Radio/Location-ID; otherwise, this field displays as hyphen (-).
Neighbor AP/MAC/Location-ID	Name, MAC address, and location ID of a neighboring AP. **NOTE** If APs are named based on their locations, this field displays as AP name/MAC/Radio/Location-ID; otherwise, this field displays as hyphen (-).
RSSI	RSSI of a neighboring AP.
Update Time	Time when RSSI information is collected.

11.14.6 display references mesh-handover-profile

Function

The **display references mesh-handover-profile** command displays information about Mesh profiles by which a specified Mesh handover profile is referenced.

Format

display references mesh-handover-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays information about the Mesh profiles by which a specified Mesh handover profile is referenced.	The Mesh handover profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references mesh-handover-profile** command to check the Mesh profiles by which a Mesh handover profile is referenced.

Example

Display information about Mesh profiles by which the Mesh handover profile **test** is referenced.

```
<HUAWEI> display references mesh-handover-profile name test
--------------------------------------------------------------------------------
Reference type              Reference name
--------------------------------------------------------------------------------
Mesh profile                profile-1
Mesh profile                profile-2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-275 Description of the **display references mesh-handover-profile** command output

Item	Description
Reference type	Type of the profile by which a Mesh handover profile is referenced. A Mesh handover profile can only be referenced by a Mesh profile.
Reference name	Name of the profile by which a Mesh handover profile is referenced. To configure this parameter, run the **mesh-handover-profile (Mesh profile view)** command in the Mesh profile view.

11.14.7 doppler-optimize disable

Function

The **doppler-optimize disable** command disables the Doppler optimization function in a Mesh handover scenario.

The **undo doppler-optimize disable** command enables the Doppler optimization function in a Mesh handover scenario.

By default, the Doppler optimization function is enabled in a Mesh handover scenario.

Format

doppler-optimize disable

undo doppler-optimize disable

Parameters

None

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Doppler optimization function reduces the impact of the Doppler effect on radio signals in vehicle-ground communication scenarios, thereby improving air interface performance.

Precautions

In Mesh vehicle-ground communication scenarios, it is recommended that the Doppler optimization function be disabled when vehicles are stationary to prevent impact on air interface performance.

Example

Disable the Doppler optimization function in a Mesh handover scenario.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] doppler-optimize disable
```


11.14.8 doppler-optimize level

Function

The **doppler-optimize level** command configures the Doppler optimization mode in a Mesh handover scenario.

The **undo doppler-optimize level** command restores the default Doppler optimization mode in a Mesh handover scenario.

The default Doppler optimization mode is low in a Mesh handover scenario.

Format

doppler-optimize level { **low** | **medium** }

undo doppler-optimize level

Parameters

Parameter	Description	Value
low	Sets the Doppler optimization mode to low. This configuration is recommended when the average vehicle speed is less than or equal to 80 km/h.	-
medium	Sets the Doppler optimization mode to medium. This configuration is recommended when the average vehicle speed is greater than 80 km/h.	-

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

The Doppler optimization function reduces the impact of the Doppler effect on radio signals in vehicle-ground communication scenarios, thereby improving air interface performance.

In practice, the Doppler optimization mode needs to be adjusted based on the main speed range of vehicles.

Example

Set the Doppler optimization mode to medium.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] doppler-optimize level medium
```

11.14.9 hal half-band disable

Function

The **hal half-band disable** command disables the half-band function on AP radios.

The **undo hal half-band disable** command enables the half-band function on AP radios.

By default, the half-band function is enabled on AP radios.

Format

hal half-band disable

undo hal half-band disable

Parameters

None

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

In vehicle-ground communication Mesh handover scenarios, some RF ports on an AP may have no antennas installed. In this case, information on these ports will be lost when information is transmitted based on the half-band algorithm, deteriorating performance. To address this issue, you can run this command to disable the half-band function.

Example

Disable the half-band function on AP radios.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] hal half-band disable
```


11.14.10 location-based-algorithm enable

Function

The **location-based-algorithm enable** command enables the location-based enhanced link handover algorithm.

The **undo location-based-algorithm enable** command disables the location-based enhanced link handover algorithm.

By default, the location-based enhanced link handover algorithm is disabled.

Format

location-based-algorithm enable

undo location-based-algorithm enable

Parameters

None

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

After the location-based enhanced link handover algorithm is enabled, the vehicle-mounted AP will switch the active link to the nearest trackside AP that meets handover requirements.

In vehicle-ground communication scenarios, signals of a trackside AP distant from a train may be temporarily better than the trackside AP near the train due to radio environment changes. If an active link handover occurs at this time, the active link may be incorrectly switched to the distant trackside AP. To prevent incorrect handovers and improve vehicle-ground communication quality, you can use the location-based enhanced link handover algorithm. This algorithm requires that trackside APs be named in ascending or descending order of sequence numbers.

Trackside APs should be named in *head-name_sequence-number* format. *head-name* describes track line information and can be different for trackside APs on the same track. It is recommended that you set the same *head-name* for APs on a track to differentiate tracks. *sequence-number* of APs along a track must be in descending or ascending order. The sequence numbers of trackside APs can be set with unequal steps. *head-name* and *sequence-number* are separated using an underscore (_), for example, L1_001, L1_002, L1_005, L1_010.

Example

Enable the location-based enhanced link handover algorithm.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] location-based-algorithm enable
```

11.14.11 link-probe-interval

Function

The **link-probe-interval** command sets a Mesh link probe interval in a Mesh handover profile.

The **undo link-probe-interval** command restores the default Mesh link probe interval in a Mesh handover profile.

By default, the Mesh link probe interval is 100 ms in a Mesh handover profile.

Format

link-probe-interval *value*

undo link-probe-interval

Parameters

Parameter	Description	Value
value	Specifies the interval for detecting Mesh links.	The value is an integer that ranges from 50 to 6000, in milliseconds. The default value is 100.

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

In vehicle-ground communication scenarios, a trackside AP periodically sends unicast probe frames to detect RSSIs of Mesh links and executes the handover algorithm based on the detection result. A larger interval delays link handover, interrupting vehicle-ground communications. A smaller interval increases air port costs and burden. Therefore, you need to configure a proper interval for detecting Mesh links according to train operating conditions.

Precautions

You are advised to set the same Mesh link probe interval for vehicle-mounted APs and trackside APs.

Example

Set the Mesh link probe interval to 150 ms in the Mesh handover profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] link-probe-interval 150
```

11.14.12 mesh-handover-profile

Function

The **mesh-handover-profile** command creates a Mesh handover profile or displays the Mesh handover profile view.

The **undo mesh-handover-profile** command deletes a Mesh handover profile.

By default, the system provides the Mesh handover profile **default**.

Format

mesh-handover-profile name *profile-name*

undo mesh-handover-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Mesh handover profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all Mesh handover profiles. **NOTE** The Mesh handover profile **default** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After a Mesh handover profile is bound to a Mesh profile, the Mesh profile can provide the vehicle-ground fast link handover function and apply to vehicle-ground communication scenarios.

Example

Create the Mesh handover profile **handover** and bind it to the Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name handover
[HUAWEI-wlan-mesh-handover-handover] quit
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] mesh-handover-profile handover
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.14.13 mesh-handover-profile (Mesh profile view)

Function

The **mesh-handover-profile** command binds a Mesh handover profile to a Mesh profile.

The **undo mesh-handover-profile** command unbinds a Mesh handover profile from a Mesh profile.

By default, no Mesh handover profile is bound to a Mesh profile.

Format

mesh-handover-profile *profile-name*

undo mesh-handover-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the Mesh handover profile bound to a Mesh profile.	The Mesh handover profile must exist.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **mesh-handover-profile** command to bind a Mesh handover profile to a Mesh profile so that the Mesh profile can provide the vehicle-ground fast link handover function and apply to vehicle-ground communication scenarios.

Example

Create the Mesh handover profile **handover** and bind it to the Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name handover
[HUAWEI-wlan-mesh-handover-handover] quit
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] mesh-handover-profile handover
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.15 Hotspot 2.0 Configuration Commands

NOTE

Hotspot 2.0 is not supported by the following APs.

- AirEngine 9700D-S (including matching ORUs)
- AirEngine X77X
- AirEngine X76X

11.15.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.15.2 cellular-network-profile

Function

The **cellular-network-profile** command creates a cellular network profile or displays the view of an existing cellular network profile.

The **undo cellular-network-profile** command deletes a cellular network profile.

By default, no cellular network profile exists in the system.

Format

cellular-network-profile name *profile-name*

undo cellular-network-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a cellular network profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Delete all cellular network profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot 2.0 services on cellular networks. When connecting to the networks, user terminals can obtain network information from APs, which helps them to select desired networks.

Follow-up Procedure

Run the **plmn-id** command to configure the PLMN identifier and run the **cellular-network-profile (Hotspot2.0 profile view)** command to bind the cellular network profile to a Hotspot2.0 profile to make the cellular network profile take effect.

Example

Create the cellular network profile **cellular-network-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] cellular-network-profile name cellular-network-profile1
[HUAWEI-wlan-cellular-net-cellular-network-profile1]
```


11.15.3 cellular-network-profile (Hotspot2.0 profile view)

Function

The **cellular-network-profile** command binds a cellular network profile to a Hotspot2.0 profile.

The **undo cellular-network-profile** command unbinds a cellular network profile from a Hotspot2.0 profile.

By default, no cellular network profile is bound to a Hotspot2.0 profile.

Format

cellular-network-profile *profile-name*

undo cellular-network-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a cellular network profile.	The cellular network profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot 2.0 services on a cellular network. When connecting to the network, user terminals need to obtain the cellular network identifier (3GPP Cellular PLMN) from APs to select desired networks. You can run the **cellular-network-profile** command to create a cellular network profile and the **plmn-id** command to configure the Public Land Mobile Network (PLMN) identifier of the network operator, and then bind the cellular network profile to a Hotspot 2.0 profile to make the configuration take effect.

Example

Bind cellular network profile **cellular-network-profile1** to the Hotspot 2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] cellular-network-profile cellular-network-profile1
```


11.15.4 connection-capability-profile

Function

The **connection-capability-profile** command creates a connection capability profile or displays the view of an existing connection capability profile.

The **undo connection-capability-profile** command deletes a connection capability profile.

By default, no connection capability profile exists in the system.

Format

connection-capability-profile name *profile-name*

undo connection-capability-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a connection capability profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all connection capability profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services for networks. When user terminals connect to the networks, they can obtain network connection capability information from APs, including allowed protocols and ports, which helps them to select desired networks.

Follow-up Procedure

Run the **connection-capability-profile (Hotspot2.0 profile view)** command to bind the connection capability profile to a Hotspot2.0 profile so that the connection capability profile can take effect.

Example

Create the connection capability profile **connection-capability-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] connection-capability-profile name connection-capability-profile1
[HUAWEI-wlan-co-cap-prof-connection-capability-profile1]
```

11.15.5 connection-capability-profile (Hotspot2.0 profile view)

Function

The **connection-capability-profile** command binds a connection capability profile to a Hotspot2.0 profile.

The **undo connection-capability-profile** command unbinds a connection capability profile from a Hotspot2.0 profile.

By default, no connection capability profile is bound to a Hotspot2.0 profile.

Format

connection-capability-profile *profile-name*

undo connection-capability-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a connection capability profile.	The connection capability profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services for networks. When user terminals connect to the networks, they can obtain network connection capability information from APs, including allowed protocols and ports, which helps them to select desired networks. You can run the **connection-capability-profile** command to create a connection capability profile and run the **connection-capability** command to set whether networks support specific IP protocols and ports. After that, you bind the connection capability profile to a Hotspot2.0 profile.

Example

Bind the connection capability profile **connection-capability-profile1** to the Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] connection-capability-profile connection-capability-profile1
```

11.15.6 connection-capability

Function

The **connection-capability** command sets whether Hotspot2.0 networks support common IP protocols and ports.

The **undo connection-capability** command restores the default setting.

By default, no supported protocol is specified in a connection capability profile.

Format

connection-capability { **esp** | **icmp** | **tcp-ftp** | **tcp-http** | **tcp-pptp-vpn** | **tcp-ssh** | **tcp-tls-vpn** | **tcp-voip** | **udp-ike2-4500** | **udp-ike2-500** | **udp-voip** } { **on** | **off** }

undo connection-capability { **esp** | **icmp** | **tcp-ftp** | **tcp-http** | **tcp-pptp-vpn** | **tcp-ssh** | **tcp-tls-vpn** | **tcp-voip** | **udp-ike2-4500** | **udp-ike2-500** | **udp-voip** }

Parameters

Parameter	Description	Value
esp	Sets the supported protocol to ESP and port number to 0.	-
icmp	Sets the supported protocol to ICMP and port number to 0.	-
tcp-ftp	Sets the supported protocol to FTP and port number to 20. FTP is not a secure protocol, and it is not recommended.	-

Parameter	Description	Value
tcp-http	Sets the supported protocol to HTTP and port number to 80. HTTP is not a secure protocol, and it is not recommended.	-
tcp-pptp-vpn	Sets the protocol for VPN services to PPTP and port number to 1723.	-
tcp-ssh	Sets the supported protocol to SSH.	-
tcp-tls-vpn	Sets the supported protocol to the TLS VPN protocol and port number to 443.	-
tcp-voip	Sets the supported protocol to the TCP VoIP protocol and port number to 5060.	-
udp-ike2-4500	Sets the supported protocol to the IKEv2 protocol and port number to 4500.	-
udp-ike2-500	Sets the supported protocol to the IKEv2 protocol and port number to 500.	-
udp-voip	Sets the supported protocol to the UDP VoIP protocol and port number to 5060.	-
on	Supports specified IP protocols and ports.	-
off	Indicates that specified IP protocols and ports are not supported.	-

Views

Connection capability profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **connection-capability** command to set whether Hotspot2.0 networks support common IP protocols and ports.

You can use the **connection-capability** command to set multiple supported protocols at the same time.

Example

Set the supported protocol to ICMP.

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



```
[HUAWEI-wlan-view] connection-capability-profile name connection-capability-profile1
[HUAWEI-wlan-co-cap-prof-connection-capability-profile1] connection-capability icmp on
```

11.15.7 display cellular-network-profile

Function

The **display cellular-network-profile** command displays information about a cellular network profile.

Format

display cellular-network-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all cellular network profiles.	-
name *profile-name*	Displays information about a specified cellular network profile.	The cellular network profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cellular-network-profile** command to view information about cellular network profiles.

Example

Display information about all cellular network profiles.

```
<HUAWEI> display cellular-network-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
cellular-network-profile1          1
--------------------------------------------------------------------------------
Total: 1
```


Table 11-276 Description of the **display cellular-network-profile all** command output

Item	Description
Profile name	Name of a cellular network profile.
Reference	Number of times a cellular network profile is referenced.

Display information about the cellular network profile **cellular-network-profile1**.

```
<HUAWEI> display cellular-network-profile name cellular-network-profile1
--------------------------------------------------------------------------------
Index     PLMN ID
--------------------------------------------------------------------------------
0         10001
--------------------------------------------------------------------------------
Total: 1
```

Table 11-277 Description of the **display cellular-network-profile name** *profile-name* command output

Item	Description
Index	Index.
PLMN ID	Public land mobile network (PLMN) ID. To configure this parameter, run the **plmn-id** command.

11.15.8 display connection-capability-profile

Function

The **display connection-capability-profile** command displays information about a connection capability profile.

Format

display connection-capability-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all connection capability profiles.	-

Parameter	Description	Value
name *profile-name*	Displays information about a specified connection capability profile.	The connection capability profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display connection-capability-profile** command to view information about connection capability profiles.

Example

Display information about all connection capability profiles.

```
<HUAWEI> display connection-capability-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
connection-capability-profile1      1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-278 Description of the **display connection-capability-profile all** command output

Item	Description
Profile name	Name of a connection capability profile.
Reference	Number of times a connection capability profile is referenced.

Display information about the connection capability profile **connection-capability-profile1**.

```
<HUAWEI> display connection-capability-profile name connection-capability-profile1
--------------------------------------------------------------------------------
ESP                 : -
ICMP                : on
TCP-FTP             : -
TCP-HTTP            : -
TCP-PPTP-VPN        : -
TCP-SSH             : -
TCP-TLS-VPN         : -
TCP-VoIP            : -
```



```
UDP-IKEv2 port 4500    : -
UDP-IKEv2 port 500     : -
UDP-VoIP               : -
------------------------------------------------------------------------------
```

Table 11-279 Description of the **display connection-capability-profile name** *profile-name* command output

Item	Description
ESP	Whether ESP (port number 0) is supported. To configure this parameter, run the **connection-capability** command.
ICMP	Whether ICMP (port number 0) is supported. To configure this parameter, run the **connection-capability** command.
TCP-FTP	Whether FTP (port number 20) is supported. To configure this parameter, run the **connection-capability** command.
TCP-HTTP	Whether HTTP (port number 80) is supported. To configure this parameter, run the **connection-capability** command.
TCP-PPTP-VPN	Whether PPTP for VPN services (port number 1723) is supported. To configure this parameter, run the **connection-capability** command.
TCP-SSH	Whether SSH is supported. To configure this parameter, run the **connection-capability** command.
TCP-TLS-VPN	Whether TLS VPN (port number 443) is supported. To configure this parameter, run the **connection-capability** command.
TCP-VoIP	Whether TCP VoIP (port number 5060) is supported. To configure this parameter, run the **connection-capability** command.
UDP-IKEv2 port 4500	Whether IKEv2 (port number 4500) is supported. To configure this parameter, run the **connection-capability** command.

Item	Description
UDP-IKEv2 port 500	Whether IKEv2 (port number 500) is supported. To configure this parameter, run the **connection-capability** command.
UDP-VoIP	Whether UDP VoIP (port number 5060) is supported. To configure this parameter, run the **connection-capability** command.

11.15.9 display hotspot2-profile

Function

The **display hotspot2-profile** command displays the Hotspot 2.0 profile configuration.

Format

display hotspot2-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Hotspot 2.0 profile.	The Hotspot 2.0 profile must exist.
all	Displays all Hotspot 2.0 profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot 2.0 services, you can run this command to view the Hotspot 2.0 profile configuration.

Example

Display all Hotspot 2.0 profiles on the device.

```
<HUAWEI> display hotspot2-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
hotspot                         1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-280 Description of the **display hotspot2-profile all** command output

Item	Description
Profile name	Name of a Hotspot 2.0 profile.
Reference	Number of times a Hotspot 2.0 profile is referenced.

Display the configuration of the Hotspot 2.0 profile **hotspot**.

```
<HUAWEI> display hotspot2-profile name hotspot
--------------------------------------------------------------------------------
Network type                    : public-free
Internet access                 : enable
Venue group code                : 3
Venue type code                 : 3
HESSID                          : 00e0-fc50-89e0
IPv4 address availability       : available
IPv6 address availability       : available
Network authentication type     : online-enroll
Redirect URL                    :
P2P information element         : disable
cellular-network-profile        : cellular-network-profile1
connection-capability-profile   : connection-capability-profile1
operator-name-profile           : operator-name-profile1
operating-class-profile         : operating-class-profile1
operator-domain-profile         : operator-domain-profile1
NAI-realm-profile               : nai-realm-profile1
venue-name-profile              : venue-name-profile1
roaming-consortium-profile      : roaming-consortium-profile1
--------------------------------------------------------------------------------
```

Table 11-281 Description of the **display hotspot2-profile name** *profile-name* command output

Item	Description
Network type	Type of a Hotspot 2.0 network. To configure this parameter, run the **network-authen-type** command.
Internet access	Whether a Hotspot 2.0 network supports Internet access. To configure this parameter, run the **network-authen-type** command.

Item	Description
Venue group code	Venue group code of a Hotspot 2.0 network. To configure this parameter, run the **venue-type** command.
Venue type code	Venue type code of a Hotspot 2.0 network. To configure this parameter, run the **venue-type** command.
HESSID	HESSID of a Hotspot 2.0 network. To configure this parameter, run the **hessid** command.
IPv4 address availability	Types of IPv4 addresses on a Hotspot 2.0 network. To configure this parameter, run the **ipv4-address-avail** command.
IPv6 address availability	Types of IPv6 addresses on a Hotspot 2.0 network. To configure this parameter, run the **ipv6-address-avail** command.
Network authentication type	Hotspot 2.0 network authentication type. To configure this parameter, run the **network-authen-type** command.
Redirect URL	Redirection URL if the Hotspot 2.0 network authentication type is set to Portal authentication. To configure this parameter, run the **network-authen-type** command.
P2P information element	Whether a Hotspot 2.0 network allows for cross connections between P2P devices. To configure this parameter, run the **p2p-cross-connect disable** command.
cellular-network-profile	Cellular network profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **cellular-network-profile (Hotspot 2.0 profile view)** command.

Item	Description
connection-capability-profile	Connection capability profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **connection-capability-profile (Hotspot 2.0 profile view)** command.
operator-name-profile	Operator name profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **operator-name-profile (Hotspot 2.0 profile view)** command.
operating-class-profile	Operating class profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **operating-class-profile (Hotspot 2.0 profile view)** command.
operator-domain-profile	Operator domain profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **operator-domain-profile (Hotspot 2.0 profile view)** command.
NAI-realm-profile	NAI realm profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **nai-realm-profile (Hotspot 2.0 profile view)** command.
venue-name-profile	Venue name profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **venue-name-profile (Hotspot 2.0 profile view)** command.
roaming-consortium-profile	Roaming consortium profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **roaming-consortium-profile (Hotspot 2.0 profile view)** command.

11.15.10 display nai-realm-profile

Function

The **display nai-realm-profile** command displays the configuration of a NAI realm profile.

Format

display nai-realm-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays all NAI realm profiles.	-
name *profile-name*	Displays the configuration of a specified NAI realm profile.	The NAI realm profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view the configuration of NAI realm profiles.

Example

Display the configuration of all NAI realm profiles.

```
<HUAWEI> display nai-realm-profile all
-------------------------------------------------------------
Profile name        Reference
-------------------------------------------------------------
nai-realm-profile1  1
-------------------------------------------------------------
Total: 1
```

Table 11-282 Description of the **display nai-realm-profile all** command output

Item	Description
Profile name	Name of a NAI realm profile.
Reference	Number of times a NAI realm profile is referenced.

Display the configuration of the NAI realm profile **nai-realm-profile1**.

```
<HUAWEI> display nai-realm-profile name nai-realm-profile1
-------------------------------------------------------------------------------
Index           Method              ID/Parameter        Realm-name
-------------------------------------------------------------------------------
0               All                 -/-                 attwireless.com
-------------------------------------------------------------------------------
```


Table 11-283 Description of the **display nai-realm-profile name** *profile-name* command output

Item	Description
Index	Index of a NAI realm member.
Method	Extensible Authentication Protocol (EAP) authentication method of a NAI realm. To configure this parameter, run the **nai-realm** command.
ID/Parameter	EAP authentication ID and parameters of a NAI realm. To configure this parameter, run the **nai-realm** command.
Realm-name	Name of a NAI realm. To configure this parameter, run the **nai-realm** command.

11.15.11 display operating-class-profile

Function

The **display operating-class-profile** command displays the configuration of an operating class profile.

Format

display operating-class-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays the configuration of all operating class profiles.	-
name *profile-name*	Displays the configuration of a specified operating class profile.	The operating class profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view the configuration of operating class profiles.

Example

Display the configuration of all operating class profiles.

```
<HUAWEI> display operating-class-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
operating-class-profile1          1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-284 Description of the **display operating-class-profile all** command output

Item	Description
Profile name	Name of an operating class profile.
Reference	Number of times an operating class profile is referenced.

Display the configuration of the operating class profile **operating-class-profile1**.

```
<HUAWEI> display operating-class-profile name operating-class-profile1
--------------------------------------------------------------------------------
Operating class indication:
95
--------------------------------------------------------------------------------
Total: 1
```

Table 11-285 Description of the **display operating-class-profile name** *profile-name* command output

Item	Description
Operating class indication	Operating class indication configured in the profile. To configure this parameter, run the **operating-class-indication** command.

11.15.12 display operator-domain-profile

Function

The **display operator-domain-profile** command displays the configuration of an operator domain profile.

Format

display operator-domain-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays the configuration of all operator domain profiles.	-
name *profile-name*	Displays the configuration of a specified operator domain profile.	The operator domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view the configuration of operator domain profiles.

Example

Display the configuration of all operator domain profiles.

```
<HUAWEI> display operator-domain-profile all
-------------------------------------------------------------
Profile name                Reference
-------------------------------------------------------------
operator-domain-profile1    1
-------------------------------------------------------------
Total: 1
```

Table 11-286 Description of the **display operator-domain-profile all** command output

Item	Description
Profile name	Name of an operator domain profile
Reference	Number of times an operator domain profile is referenced.

Display the configuration of the operator domain profile **operator-domain-profile1**.

```
<HUAWEI> display operator-domain-profile name operator-domain-profile1
-------------------------------------------------------------
```

```
Index                    Domain name
-------------------------------------------------------------
0                        attwireless.com
-------------------------------------------------------------
```

Table 11-287 Description of the **display operator-domain-profile name** *profile-name* command output

Item	Description
Index	Index of an operator domain
Domain name	Name of an operator domain. To configure this parameter, run the **domain-name** command.

11.15.13 display operator-name-profile

Function

The **display operator-name-profile** command displays information about an operator name profile.

Format

display operator-name-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all operator name profiles.	-
name *profile-name*	Displays information about a specified operator name profile.	The operator name profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display operator-name-profile** command to view information about an operator name profile.

Example

Display information about all operator name profiles.

```
<HUAWEI> display operator-name-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
operator-name-profile1          1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-288 Description of the **display operator-name-profile all** command output

Item	Description
Profile name	Name of an operator name profile.
Reference	Number of times an operator name profile is referenced.

Display information about the operator name profile **operator-name-profile1**.

```
<HUAWEI> display operator-name-profile name operator-name-profile1
--------------------------------------------------------------------------------
Index           Language-code           Name
--------------------------------------------------------------------------------
0               en                      att
--------------------------------------------------------------------------------
```

Table 11-289 Description of the **display operator-name-profile name** *profile-name* command output

Item	Description
Index	Index of a friendly operator name.
Language-code	Language type. To configure this parameter, run the **operator-friendly-name** command.
Name	Friendly operator name. To configure this parameter, run the **operator-friendly-name** command.

11.15.14 display references cellular-network-profile

Function

The **display references cellular-network-profile** command displays reference information about a cellular network profile.

Format

display references cellular-network-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified cellular network profile.	The cellular network profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references cellular-network-profile** command to view reference information about a cellular network profile.

Example

Display reference information about the cellular network profile **cellular-network-profile1**.

```
<HUAWEI> display references cellular-network-profile name cellular-network-profile1
--------------------------------------------------------------------------------
Reference type                  Reference name
--------------------------------------------------------------------------------
hotspot2-profile                hotspot
--------------------------------------------------------------------------------
Total: 1
```

Table 11-290 Description of the **display references cellular-network-profile** command output

Item	Description
Reference type	Type of the profile to which the cellular network profile is bound.
Reference name	Name of the profile to which the cellular network profile is bound.

11.15.15 display references connection-capability-profile

Function

The **display references connection-capability-profile** command displays reference information about a connection capability profile.

Format

display references connection-capability-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified connection capability profile.	The connection capability profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references connection-capability-profile** command to view reference information about a connection capability profile.

Example

Display reference information about the connection capability profile **connection-capability-profile1**.

```
<HUAWEI> display references connection-capability-profile name connection-capability-profile1
--------------------------------------------------------------------------------
Reference type                  Reference name
--------------------------------------------------------------------------------
hotspot2-profile                hotspot
--------------------------------------------------------------------------------
Total: 1
```

Table 11-291 Description of the **display references connection-capability-profile** command output

Item	Description
Reference type	Type of the profile to which the connection capability profile is bound.

Item	Description
Reference name	Name of the profile to which the connection capability profile is bound.

11.15.16 display references hotspot2-profile

Function

The **display references hotspot2-profile** command displays reference information about a Hotspot2.0 profile.

Format

display references hotspot2-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Hotspot2.0 profile.	The Hotspot2.0 profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view reference information about a Hotspot2.0 profile.

Example

Display reference information about the Hotspot2.0 profile **hotspot**.

```
<HUAWEI> display references hotspot2-profile name hotspot
------------------------------------------------------------------------
Reference type                Reference name
------------------------------------------------------------------------
VAP profile                   vap-profile1
------------------------------------------------------------------------
Total:1
```


Table 11-292 Description of the **display references hotspot2-profile name** *profile-name* command output

Item	Description
Reference type	Type of the profile to which the Hotspot2.0 profile is bound. • VAP profile. To configure it, run the **hotspot2-profile (VAP profile view)** command.
Reference name	Name of the profile to which the Hotspot2.0 profile is bound. To configure it, run the **hotspot2-profile (VAP profile view)** command.

11.15.17 display references nai-realm-profile

Function

The **display references nai-realm-profile** command displays reference information about a NAI realm profile.

Format

display references nai-realm-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified NAI realm profile.	The NAI realm profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a NAI realm profile.

Example

Display reference information about the NAI realm profile **nai-realm-profile1**.

```
<HUAWEI> display references nai-realm-profile name nai-realm-profile1
-------------------------------------------------------------------------------
Reference type      Reference name
-------------------------------------------------------------------------------
hotspot2-profile    hotspot
-------------------------------------------------------------------------------
Total: 1
```

Table 11-293 Description of the **display references nai-realm-profile** command output

Item	Description
Reference type	Type of the profile to which the NAI realm profile is bound.
Reference name	Name of the profile to which the NAI realm profile is bound.

11.15.18 display references operating-class-profile

Function

The **display references operating-class-profile** command displays reference information about an operating class profile.

Format

display references operating-class-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	# Display reference information about a specified operating class profile.	The operating class profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about an operating class profile.

Example

Display reference information about the operating class profile **operating-class-profile1**.

```
<HUAWEI> display references operating-class-profile name operating-class-profile1
--------------------------------------------------------------------------------
Reference type       Reference name
--------------------------------------------------------------------------------
hotspot2-profile     hotspot
--------------------------------------------------------------------------------
Total: 1
```

Table 11-294 Description of the **display references operating-class-profile** command output

Item	Description
Reference type	Type of the profile to which the operating class profile is bound.
Reference name	Name of the profile to which the operating class profile is bound.

11.15.19 display references operator-domain-profile

Function

The **display references operator-domain-profile** command displays reference information about an operator domain profile.

Format

display references operator-domain-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified operator domain profile.	The operator domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about an operator domain profile.

Example

Display reference information about the operator domain profile **operator-domain-profile1**.

```
<HUAWEI> display references operator-domain-profile name operator-domain-profile1
--------------------------------------------------------------------------------
Reference type       Reference name
--------------------------------------------------------------------------------
hotspot2-profile     hotspot
--------------------------------------------------------------------------------
Total: 1
```

Table 11-295 Description of the **display references operator-domain-profile** command output

Item	Description
Reference type	Type of the profile to which the operator domain profile is bound.
Reference name	Name of the profile to which the operator domain profile is bound.

11.15.20 display references operator-name-profile

Function

The **display references operator-name-profile** command displays reference information about an operator name profile.

Format

display references operator-name-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified operator name profile.	The operator name profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references operator-name-profile** command to view reference information about an operator name profile.

Example

Display reference information about the operator name profile **operator-name-profile1**.

```
<HUAWEI> display references operator-name-profile name operator-name-profile1
------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------
hotspot2-profile            hotspot
------------------------------------------------------------------------
Total:1
```

Table 11-296 Description of the **display references operator-name-profile** command output

Item	Description
Reference type	Type of the profile to which the operator name profile is bound.
Reference name	Name of the profile to which the operator name profile is bound.

11.15.21 display references roaming-consortium-profile

Function

The **display references roaming-consortium-profile** command displays reference information about a roaming consortium profile.

Format

display references roaming-consortium-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a roaming consortium profile.	The roaming consortium profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view reference information about a roaming consortium profile.

Example

Display reference information about the roaming consortium profile **roaming-consortium-profile1**.

```
<HUAWEI> display references roaming-consortium-profile name roaming-consortium-profile1
------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------
hotspot2-profile            hotspot
------------------------------------------------------------------------
Total:1
```

Table 11-297 Description of the **display references roaming-consortium-profile name** *profile-name* command output

Item	Description
Reference type	Type of the profile to which the roaming consortium profile is bound. • hotspot2-profile: Hotspot2.0 profile. To configure it, run the **roaming-consortium-profile (Hotspot2.0 profile view)** command.
Reference name	Name of the profile to which the roaming consortium profile is bound. To configure it, run the **roaming-consortium-profile (Hotspot2.0 profile view)** command.

11.15.22 display references venue-name-profile

Function

The **display references venue-name-profile** command displays reference information about a venue name profile.

Format

display references venue-name-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a venue name profile.	The venue name profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view reference information about a venue name profile.

Example

Display reference information about the venue name profile **venue-name-profile1**.

```
<HUAWEI> display references venue-name-profile name venue-name-profile1
------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------
hotspot2-profile            hotspot
------------------------------------------------------------------------
Total:1
```


Table 11-298 Description of the **display references venue-name-profile name** *profile-name* command output

Item	Description
Reference type	Type of the profile to which the venue name profile is bound. • hotspot2-profile: Hotspot2.0 profile. To configure it, run the **venue-name-profile (Hotspot2.0 profile view)** command.
Reference name	Name of the profile to which the venue name profile is bound. To configure it, run the **venue-name-profile (Hotspot2.0 profile view)** command.

11.15.23 display roaming-consortium-profile

Function

The **display roaming-consortium-profile** command displays the configuration of a roaming consortium profile.

Format

display roaming-consortium-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a roaming consortium profile.	The roaming consortium profile must exist.
all	Displays the configuration of all roaming consortium profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view the configuration of a roaming consortium profile.

Example

Display the configuration of all roaming consortium profiles on a device.

```
<HUAWEI> display roaming-consortium-profile all
-------------------------------------------------------------------------------
Profile name                    Reference
-------------------------------------------------------------------------------
roaming-consortium-profile1     1
-------------------------------------------------------------------------------
Total: 1
```

Table 11-299 Description of the **display roaming-consortium-profile all** command output

Item	Description
Profile name	Name of a roaming consortium profile.
Reference	Number of times a roaming consortium profile is referenced.

Display the configuration of the roaming consortium profile **roaming-consortium-profile1**.

```
<HUAWEI> display roaming-consortium-profile name roaming-consortium-profile1
-------------------------------------------------------------------------------
Index    Roaming consortium OI    In beacon
-------------------------------------------------------------------------------
0        00-11-22                 Y
-------------------------------------------------------------------------------
Total: 1
```

Table 11-300 Description of the **display roaming-consortium-profile name** *profile-name* command output

Item	Description
Index	Index of a roaming consortium member.
Roaming consortium OI	OI of a roaming consortium member. To configure this parameter, run the **roaming-consortium-oi** command.

Item	Description
In beacon	Whether Beacon and Probe Response frames sent from APs carry OIs of roaming consortium members. • Y: Yes • N: No To configure this parameter, run the **roaming-consortium-oi** command.

11.15.24 display venue-name-profile

Function

The **display venue-name-profile** command displays the configuration of a venue name profile.

Format

display venue-name-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a venue name profile.	The venue name profile must exist.
all	Displays the configuration of all venue name profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view the configuration of venue name profiles.

Example

Display the configuration of all venue name profiles on a device.

```
<HUAWEI> display venue-name-profile all
------------------------------------------------------------------------------
Profile name                    Reference
------------------------------------------------------------------------------
venue-name-profile1             1
------------------------------------------------------------------------------
Total: 1
```

Table 11-301 Description of the **display venue-name-profile all** command output

Item	Description
Profile name	Name of a venue name profile.
Reference	Number of times a venue name profile is referenced.

Display the configuration of the venue name profile **venue-name-profile1**.

```
<HUAWEI> display venue-name-profile name venue-name-profile1
------------------------------------------------------------------------------
Index           Language code           Name
------------------------------------------------------------------------------
0               en                      CenterStation
------------------------------------------------------------------------------
```

Table 11-302 Description of the **display venue-name-profile name** *profile-name* command output

Item	Description
Index	Index of venue name information.
Language code	Language type. To configure this parameter, run the **venue-name** command.
Name	Venue name. To configure this parameter, run the **venue-name** command.

11.15.25 domain-name

Function

The **domain-name** command configures a domain name for a hotspot operator.

The **undo domain-name** command deletes the domain name of a hotspot operator.

By default, no domain name is configured for a hotspot operator.

Format

domain-name *domain-name*

undo domain-name *domain-name*

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name of a hotspot operator.	The value is a string of 1 to 63 characters in compliance with RFC1035. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").

Views

Operator domain profile view

Default Level

2: Configuration level

Usage Guidelines

After a domain name is configured for a hotspot operator, terminals can query the domain name through ANQP to select desired networks.

Example

Configure domain name **attwireless.com** for a hotspot operator.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operator-domain-profile name operator-domain-profile1
[HUAWEI-wlan-op-domain-prof-operator-domain-profile1] domain-name attwireless.com
```

11.15.26 hessid

Function

The **hessid** command configures a Homogenous Extended Service Set Identifier (HESSID) for a Hotspot2.0 network.

The **undo hessid** command deletes an HESSID.

By default, no HESSID is configured.

Format

hessid *mac-address*

undo hessid

Parameters

Parameter	Description	Value
mac-address	Specifies an HESSID.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple Hotspot2.0 networks are available, user terminals need to identify service providers of the connected networks. An SSID is not as unique as an HESSID, which can uniquely identify APs of the same service provider. Among the APs, the BSSID of one AP is used as the HESSID. The HESSID is an optional parameter in a Hotspot2.0 profile. Beacon and Probe Response frames sent from Hotspot2.0-capable APs carry network parameter information, which helps user terminals to determine whether network parameters need to be renewed.

Precautions

If the HESSID is configured repeatedly, only the latest HESSID takes effect.

Example

Set the HESSID to **00e0-fc12-3456** in Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] hessid 00e0-fc12-3456
```


11.15.27 hotspot2-profile

Function

The **hotspot2-profile** command creates a Hotspot2.0 profile or displays the view of an existing Hotspot2.0 profile.

The **undo hotspot2-profile** command deletes a Hotspot2.0 profile.

By default, no Hotspot2.0 profile is available.

Format

hotspot2-profile name *profile-name*

undo hotspot2-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Hotspot2.0 profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all Hotspot2.0 profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure Hotspot2.0 services, create a Hotspot2.0 profile, configure network parameters in the Hotspot2.0 profile view, and bind the Hotspot2.0 profile to a VAP profile.

Follow-up Procedure

Configure the network type, roaming consortium list, and NAI realm list in the Hotspot2.0 profile and bind the Hotspot2.0 profile to a VAP profile to make the configuration take effect.

Precautions

- In a Hotspot2.0 profile, network parameters and Internet access status are mandatory and can be configured using the **network-type** command.
- Ensure that at least one of the following ANQP parameters is configured in a Hotspot2.0 profile.
  - Roaming consortium list: Run the **roaming-consortium-profile (Hotspot2.0 profile view)** command to bind a roaming consortium profile to the Hotspot2.0 profile.
  - NAI realm list: Run the **nai-realm-profile (Hotspot2.0 profile view)** command to bind a NAI realm profile to the Hotspot2.0 profile.
  - 3GPP cellular network: Run the **cellular-network-profile (Hotspot2.0 profile view)** command to bind a cellular network profile to the Hotspot2.0 profile.
- The following ANQP parameters are recommended.
  - Roaming consortium list: Run the **roaming-consortium-profile (Hotspot2.0 profile view)** command to bind a roaming consortium profile to the Hotspot2.0 profile.
  - Domain name list: Run the **operator-domain-profile (Hotspot2.0 profile view)** command to bind an operator domain profile to the Hotspot2.0 profile.

Example

Create Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot]
```

11.15.28 hotspot2-profile (VAP profile view)

Function

The **hotspot2-profile** command binds a Hotspot 2.0 profile to a VAP profile.

The **undo hotspot2-profile** command unbinds a Hotspot 2.0 profile from a VAP profile.

By default, no Hotspot 2.0 profile is bound to a VAP profile.

Format

hotspot2-profile *profile-name*

undo hotspot2-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a Hotspot 2.0 profile.	The Hotspot 2.0 profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure network parameters through Hotspot 2.0 profiles. After Hotspot 2.0 profiles are applied, STAs can obtain network information from APs and access the networks. After a Hotspot 2.0 profile is configured, bind it to a VAP profile to make the configuration take effect.

Precautions

The Hotspot 2.0 service configuration requires the authentication mode of WPA2-802.1X. Ensure that the security profile bound to the VAP profile meets this requirement.

When you perform the following operations on a VAP bound to a radio, services are interrupted:

- Bind a Hotspot 2.0 profile to the VAP profile.
- Unbind a Hotspot 2.0 profile from the VAP profile.
- Modify the parameters in a Hotspot 2.0 profile bound to the VAP profile.

Therefore, exercise caution when performing these operations.

Example

Bind the Hotspot 2.0 profile **hotspot** to the VAP profile **vap-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] hotspot2-profile hotspot
```

11.15.29 ipv4-address-avail

Function

The **ipv4-address-avail** command configures available types of IPv4 addresses on a Hotspot2.0 network.

The **undo ipv4-address-avail** command deletes available types of IPv4 addresses on a Hotspot2.0 network.

By default, no available type of IPv4 addresses is configured.

Format

ipv4-address-avail { **not-available** | **available** | **port-restricted** [**single-nat** | **double-nat**] | **private** { **single-nat** | **double-nat** } | **unknown** }

undo ipv4-address-avail

Parameters

Parameter	Description	Value
not-available	Indicates that IPv4 addresses are not available.	-
available	Indicates that IPv4 addresses are available.	-
port-restricted [**single-nat** | **double-nat**]	Indicates port restricted IPv4 addresses are available. • **single-nat**: Single-NATed and port-restricted IPv4 addresses are available. • **single-nat**: Double-NATed and port-restricted IPv4 addresses are available.	-
private { **single-nat** | **double-nat** }	Indicates that private IPv4 addresses are available. • **single-nat**: Single-NATed private IPv4 addresses are available. • **double-nat**: Double-NATed private IPv4 addresses are available.	-
unknown	Indicates that availability of the IPv4 address type is not known.	-

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When user terminals connect to a Hotspot2.0 network, Hotspot2.0 can transfer available IPv4 address types as ANQP parameters to the user terminals through

APs. In this way, the user terminals can know the IP address types they can obtain after connecting to the network.

Example

Set IPv4 addresses to **available** in hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] ipv4-address-avail available
```

11.15.30 ipv6-address-avail

Function

The **ipv6-address-avail** command configures available types of IPv6 addresses on a Hotspot 2.0 network.

The **undo ipv6-address-avail** command deletes available types of IPv6 addresses on a Hotspot 2.0 network.

By default, no available type of IPv6 addresses is configured.

Format

ipv6-address-avail { **not-available** | **available** | **unknown** }

undo ipv6-address-avail

Parameters

Parameter	Description	Value
not-available	Indicates that IPv6 addresses are not available.	-
available	Indicates that IPv6 addresses are available.	-
unknown	Indicates that the availability of IPv6 address types is not known.	-

Views

Hotspot 2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When STAs connect to a Hotspot 2.0 network, Hotspot 2.0 can transfer available IPv6 address types as ANQP parameters to the STAs through APs. In this way, the STAs can know the IPv6 address types they can obtain after connecting to the network.

Example

Configure IPv6 addresses to be available in the Hotspot 2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] ipv6-address-avail available
```

11.15.31 nai-realm-profile

Function

The **nai-realm-profile** command creates a NAI realm profile or displays the view of an existing NAI realm profile.

The **undo nai-realm-profile** command deletes a NAI realm profile.

By default, no NAI realm profile is available in the system.

Format

nai-realm-profile name *profile-name*

undo nai-realm-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a NAI realm profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all NAI realm profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A NAI realm profile is used to configure the network access identifier (NAI) realm name, authentication mode, and authentication parameters for networks accessible to users.

Example

Create NAI realm profile **nai-realm-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] nai-realm-profile name nai-realm-profile1
[HUAWEI-wlan-nai-realm-prof-nai-realm-profile1]
```

11.15.32 nai-realm-profile (Hotspot2.0 profile view)

Function

The **nai-realm-profile** command binds a NAI realm profile to a Hotspot2.0 profile.

The **undo nai-realm-profile** command unbinds a NAI realm profile from a Hotspot2.0 profile.

By default, no NAI realm profile is bound to a Hotspot2.0 profile.

Format

nai-realm-profile *profile-name*

undo nai-realm-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a NAI realm profile.	The NAI realm profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services on a non-cellular network. When connecting to the non-cellular network, user terminals can obtain service provider information of the network, including the NAI realm name and authentication mode. This facilitates terminal access. You can run the **nai-realm-profile** command to create a NAI realm profile and the **nai-realm** command in the NAI realm profile view to configure NAI realms, and then bind the NAI realm profile to a Hotspot2.0 profile to make the configuration take effect.

Example

Bind NAI realm profile **nai-realm-profile1** to Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] nai-realm-profile nai-realm-profile1
```

11.15.33 nai-realm

Function

The **nai-realm** command configures a network access identifier (NAI) realm.

The **undo nai-realm** command deletes a NAI realm.

By default, no NAI realm is configured.

Format

nai-realm realm-name *realm-name* [**eap-method-type** *eap-method-type* [**eap-authen-id** *eap-authen-id* **eap-authen-para** *eap-authen-para*]]

undo nai-realm realm-name *realm-name* [**eap-method-type** *eap-method-type* [**eap-authen-id** *eap-authen-id*]]

Parameters

Parameter	Description	Value
realm-name *realm-name*	Specifies a NAI realm name.	The value is a string of 1 to 63 characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").

Parameter	Description	Value
eap-method-type *eap-method-type*	Specifies an EAP authentication mode for a NAI realm.	Enumerated value: • eap-aka: EAP-AKA authentication • eap-sim: GSM Subscriber Identity Modules • eap-tls: EAP-TLS • eap-ttls: EAP-TTLS
eap-authen-id *eap-authen-id*	Specifies an EAP authentication ID for a NAI realm.	The value is an integer that ranges from 0 to 255.
eap-authen-para *eap-authen-para*	Specifies the EAP authentication parameter of a NAI realm.	The value is an integer that ranges from 0 to 255.

Views

NAI realm profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you configure a NAI realm, terminals can access the configured operator network.

Precautions

- If you configure the same name for NAI realms, the NAI realm with fuzzy command configuration will overwrite the NAI realm with exact command configuration.

  For example, the **nai-realm realm-name attwireless.com** command configuration will overwrite the **nai-realm realm-name attwireless.com eap-method-type eap-aka** command configuration, and the **nai-realm realm-name attwireless.com eap-method-type eap-aka** command configuration will overwrite the **nai-realm realm-name attwireless.com eap-method-type eap-aka eap-authen-id 1 eap-authen-para 1** command configuration.
- NAI realms are deleted according to the longest matching rule.

For example, the NAI realm configured using the **nai-realm realm-name attwireless.com** command cannot be deleted using the **undo nai-realm realm-name attwireless.com eap-method-type eap-aka** command.

Example

Configure NAI realm **attwireless.com**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] nai-realm-profile name nai-realm-profile1
[HUAWEI-wlan-nai-realm-prof-nai-realm-profile1] nai-realm realm-name attwireless.com
```

11.15.34 network-authen-type

Function

The **network-authen-type** command sets a network authentication type for a Hotspot2.0 profile.

The **undo network-authen-type** command deletes a network authentication type.

By default, no network authentication type is configured.

Format

network-authen-type { **acceptance** [**redirect-url** *url*] | **dns-redirection** | **http-https-redirection redirect-url** *url* | **online-enroll** }

undo network-authen-type

Parameters

Parameter	Description	Value
acceptance	Indicates acceptance of terms and conditions.	-
redirect-url *url*	Specifies the redirected URL address.	-
dns-redirection	Indicates DNS redirection.	-
http-https-redirection	Indicates HTTP and HTTPS redirection.	-
online-enroll	Indicates online enrollment.	-

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Beacon and Probe Response frames sent from Hotspot2.0-capable APs carry network parameter information, which helps user terminals to discover and select proper networks. If the network operator requests user terminals to execute specified actions, for example, opening a web page for Portal authentication, the Additional Steps Required for Access (ASRA) field must be set to 1, indicating that user terminals must implement extra authentication when connecting to a network. You can run the **network-authen-type** command to specify a network authentication type.

Example

Set the network authentication type to online enrollment in Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] network-authen-type online-enroll
```

11.15.35 network-type

Function

The **network-type** command sets a network type and Internet access status in a Hotspot2.0 profile.

The **undo network-type** command restores the default network type and Internet access status.

By default, the network type is set to **wildcard**, and Internet access is not supported.

Format

network-type { **emergency-service** | **personal-device** | **private** | **private-guest** | **public-chargeable** | **public-free** | **test** | **wildcard** } [**internet-access**]

undo network-type

Parameters

Parameter	Description	Value
emergency-service	Indicates an emergency service network.	-

Parameter	Description	Value
personal-device	Indicates a personal device network.	-
private	Indicates a private network.	-
private-guest	Indicates a private network with guest access.	-
public-chargeable	Indicates a chargeable public network.	-
public-free	Indicates a free public network.	-
test	Indicates a test network.	-
wildcard	Indicates a wildcard network.	-
internet-access	Indicates that Internet access is supported.	-

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple Hotspot2.0 networks are available, user terminals need to obtain information of each network to select the network to access. The network type and Internet access status are mandatory in a Hotspot2.0 profile. Beacon and Probe Response frames sent from Hotspot2.0-capable APs carry network parameter information, which helps user terminals to discover and select proper networks.

Precautions

If the command is executed repeatedly, only the latest configuration takes effect.

Example

Set the network type to free public network and configure the network to provide Internet access in Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] network-type public-free internet-access
```


11.15.36 operating-class-indication

Function

The **operating-class-indication** command configures an operating class indication.

The **undo operating-class-indication** command deletes an operating class indication.

By default, no operating class indication is configured in the system.

Format

operating-class-indication *operating-class-value*

undo operating-class-indication *operating-class-value*

Parameters

Parameter	Description	Value
operating-class-value	Indicates the operating class indication.	The value is an integer that ranges from 1 to 255.

Views

Operating class profile view

Default Level

2: Configuration level

Usage Guidelines

After an operating class indication is configured, users can obtain the indication through ANQP for network selection.

You can configure a maximum of 32 operating class indications using this command.

Example

Set the operating class indication to **95**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operating-class-profile name operating-class-profile1
[HUAWEI-wlan-op-class-prof-operating-class-profile1] operating-class-indication 95
```


11.15.37 operating-class-profile

Function

The **operating-class-profile** command creates an operating class profile or displays the view of an existing operating class profile.

The **undo operating-class-profile** command deletes an operating class profile.

By default, no operating class profile is configured in the system.

Format

operating-class-profile name *profile-name*

undo operating-class-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Indicates the name of the operating class profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Indicates to delete all operating class profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The operating class profile is used to configure the operating class indication of AP in on the hotspot2.0 network. When a STA accesses the network, it can obtain channel information used to access a Wi-Fi frequency from AP so that the STA can set up a connection.

Example

Create an operating class profile named **operating-class-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operating-class-profile name operating-class-profile1
[HUAWEI-wlan-op-class-prof-operating-class-profile1]
```

11.15.38 operating-class-profile (Hotspot2.0 profile view)

Function

The **operating-class-profile** command binds the specified operating class profile to a Hotspot2.0 profile view.

The **undo operating-class-profile** command unbinds the specified operating class profile from a Hotspot2.0 profile view.

By default, no operating class profile is bound to a Hotspot2.0 profile view.

Format

operating-class-profile *profile-name*

undo operating-class-profile

Parameters

Parameter	Description	Value
profile-name	Indicates the name of the operating class profile.	The value must be the name of an existing operating class profile.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA accesses a Hotspot2.0 network, it can obtain channel information used to access a Wi-Fi frequency from the AP so that the STA can set up a connection. Before binding an operating class profile to a Hotspot2.0 profile, you need to run the **operating-class-profile** command to create an operating class profile and run the **operating-class-indication** command in the profile view to configure an operating class indication.

Example

Bind the operating class profile **operating-class-profile1** to the **hotspot** profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] operating-class-profile operating-class-profile1
```

11.15.39 operator-domain-profile

Function

The **operator-domain-profile** command creates a network domain name profile or displays the view of an existing network domain name profile.

The **undo operator-domain-profile** command deletes a network domain name profile.

By default, no network domain name profile is available in the system.

Format

operator-domain-profile name *profile-name*

undo operator-domain-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Indicates the network domain name profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Indicates to delete all network domain name profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A network domain name profile is used to configure the operator domain profile. STAs can obtain the domain name information through ANQP, which is used as a basis for network selection.

Example

Create a network domain name profile named **operator-domain-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operator-domain-profile name operator-domain-profile1
[HUAWEI-wlan-op-domain-prof-operator-domain-profile1]
```

11.15.40 operator-domain-profile (Hotspot2.0 profile view)

Function

The **operator-domain-profile** command binds the specified operator domain profile to a Hotspot2.0 profile view.

The **undo operator-domain-profile** command unbinds the specified operator domain profile from a Hotspot2.0 profile view.

By default, no operator domain profile is bound to a Hotspot2.0 profile.

Format

operator-domain-profile *profile-name*

undo operator-domain-profile

Parameters

Parameter	Description	Value
profile-name	Indicates the name of the operator domain profile.	The value must be the name of an existing operator domain profile.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA accesses the Hotspot2.0 network, it can obtain the network operator domain name information from the AP so that the STA can select a network. Before binding an operator domain profile to a Hotspot2.0 profile, run the **operator-domain-profile** command to create an operator domain profile and run the **domain-name** command in the profile view to configure the operator name.

Example

Bind the operator domain profile **operator-domain-profile1** to the **hotspot** profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] operator-domain-profile operator-domain-profile1
```

11.15.41 operator-friendly-name

Function

The **operator-friendly-name** command configures the operator friendly name.

The **undo operator-friendly-name** command deletes the operator friendly name.

By default, no operator friendly name is configured in an operator name profile view.

Format

operator-friendly-name language-code *language-code* **name** *name*

undo operator-friendly-name language-code *language-code* **name** *name*

Parameters

Parameter	Description	Value
language-code *language-code*	Indicates the language.	The value is a string of 2 to 3 characters. For the value of each language, see the definition in ISO639-2 *Codes for the Representation of Names of Languages*. For example, the value is **chi**, **zho**, or **zh** for Chinese, and **eng** for English.

Parameter	Description	Value
name *name*	Indicates the operator friendly name.	The value is a string of 1 to 64 case-sensitive characters. • English venue name: The value is a string of visible characters without question marks (?) and spaces. It cannot begin or end with double quotation marks (" "). • Non-English venue name: It cannot contain half-width question marks (?). To enter a non-English venue name, ensure that the remote login terminal supports the UTF-8 encoding format; otherwise, the name cannot be displayed.

Views

Operator name profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA accesses the Hotspot2.0 network, it can obtain the operator name from the AP. This command configures the language environment names so that users can select a proper language.

If you need to enter a non-English name, you must use a tool to convert it into hexadecimal UTF-8 code.

Precautions

If you run the **operator-friendly-name** multiple times, multiple operator friendly names are configured. A maximum of 32 names can be configured.

Example

Set the operator friendly name to **operator-name-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operator-name-profile name operator-name-profile1
[HUAWEI-wlan-op-name-prof-operator-name-profile1] operator-friendly-name language-code eng name att
```

11.15.42 operator-name-profile

Function

The **operator-name-profile** command creates an operator name profile or displays the view of an existing operator name profile.

The **undo operator-name-profile** command deletes the operator name profile.

By default, no operator name profile is available in the system.

Format

operator-name-profile name *profile-name*

undo operator-name-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Indicates the name of the operator name profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Indicates to delete all operator name profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can specify different friendly names for different languages so that users can select networks.

Follow-up Procedure

Run the **operator-name-profile (Hotspot2.0 profile view)** command to apply the created operator name profile to a Hotspot2.0 profile.

Example

Create an operator name profile named **operator-name-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operator-name-profile name operator-name-profile1
[HUAWEI-wlan-op-name-prof-operator-name-profile1]
```

11.15.43 operator-name-profile (Hotspot2.0 profile view)

Function

The **operator-name-profile** command binds the specified operator name profile to a Hotspot2.0 profile view.

The **undo operator-name-profile** command unbinds the specified operator name profile from a Hotspot2.0 profile view.

By default, no operator name profile is bound to a Hotspot2.0 profile.

Format

operator-name-profile *profile-name*

undo operator-name-profile

Parameters

Parameter	Description	Value
profile-name	Indicates the name of the operator name profile.	The value must be the name of an existing operator name profile.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA accesses the Hotspot2.0 network, it can obtain the operator name from the AP. Before binding an operator name profile to a Hotspot2.0 profile, run the **operator-name-profile** command to create an operator name profile and run the **operator-friendly-name** command in the profile view to configure the operator name.

Example

Bind the operator name profile **operator-name-profile1** to the **hotspot** profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] operator-name-profile operator-name-profile1
```

11.15.44 p2p-cross-connect disable

Function

The **p2p-cross-connect disable** command configures P2P management information to prevent cross connections of P2P devices.

The **undo p2p-cross-connect disable** command deletes P2P management information.

By default, P2P management information is not configured.

Format

p2p-cross-connect disable

undo p2p-cross-connect disable

Parameters

None.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hotspot2.0 provides security measures for STAs. It prevents direct access between STAs to reduce the STA attack possibility. The P2P protocol allows direct communication between STAs; therefore, a Hotspot2.0-supported AP can add P2P management information into Beacon. In the management information, STAs are not allowed to set up P2P connections with each other.

Precautions

The **p2p-cross-connect disable** command is not recommended. An AP does not support the P2P protocol or process P2P packets; therefore, it is unnecessary to remove P2P management information from packets.

Example

Configure P2P management information in the **hotspot** profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] p2p-cross-connect disable
```

11.15.45 plmn-id

Function

The **plmn-id** command configures the Public Land Mobile Network (PLMN) identifier.

The **undo plmn-id** command deletes the PLMN identifier.

By default, no PLMN identifier is configured in the cellular network profile.

Format

plmn-id *plmn-id*

undo plmn-id *plmn-id*

Parameters

Parameter	Description	Value
plmn-id	Indicates the PLMN identifier.	The value is an integer that ranges from 10000 to 999999.

Views

Cellular network profile view

Default Level

2: Configuration level

Usage Guidelines

After the **plmn-id** command is executed, the AP notifies STAs of the operator information on the Hotspot2.0 network. The STAs can obtain the PLMN identifier to determine whether to select the cellular network according to the Hotspot2.0 network.

If you run the **plmn-id** multiple times, multiple PLMN identifiers are configured. A maximum of 32 PLMN identifiers can be configured.

Example

Set the PLMN identifier to 10001.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] cellular-network-profile name cellular-network-profile1
[HUAWEI-wlan-cellular-net-cellular-network-profile1] plmn-id 10001
```

11.15.46 roaming-consortium-oi

Function

The **roaming-consortium-oi** command configures the roaming consortium identifier of the Hotspot2.0 network.

The **undo roaming-consortium-oi** command deletes the roaming consortium identifier of the Hotspot2.0 network.

By default, no roaming consortium identifier is configured for the Hotspot2.0 network.

Format

roaming-consortium-oi *oi-value* [**in-beacon**]

undo roaming-consortium-oi *oi-value*

Parameters

Parameter	Description	Value
oi-value	Indicates the roaming consortium identifier, which is used to identify operators.	The format is HH-HH-HH or HH-HH-HH-HH-HH, in which H is in the hexadecimal format.
in-beacon	Indicates that the Beacon and probe-response frames sent by the AP contain the roaming consortium identifier.	-

Views

Roaming consortium profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If STAs may roam between the Hotspot2.0 network and a network of another operator, you can configure the OI of the operator that provides the roaming service so that STAs can select networks.

Precautions

If you run this command multiple times, multiple OIs are configured. A maximum of 32 OIs can be configured in a roaming consortium profile. To configure OIs in the roaming consortium profile, the first OI must carry the **in-beacon** parameter. A maximum of three OIs can be configured to carry the **in-beacon** parameter.

Example

Add an OI **00-11-22** to the profile **roaming-consortium-profile1** and add the OI to the Beacon and probe-response frames sent by the AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] roaming-consortium-profile name roaming-consortium-profile1
[HUAWEI-wlan-ro-co-prof-roaming-consortium-profile1] roaming-consortium-oi 00-11-22 in-beacon
```

11.15.47 roaming-consortium-profile

Function

The **roaming-consortium-profile** command creates a roaming consortium profile or displays the view of an existing roaming consortium profile.

The **undo roaming-consortium-profile** command deletes a roaming consortium profile.

By default, no roaming consortium profile is created.

Format

roaming-consortium-profile name *profile-name*

undo roaming-consortium-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a roaming consortium profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all roaming consortium profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, configure network parameters according to operator requirements. When connecting to networks, user terminals can obtain the network parameters to select desired networks. If the user terminals need to roam among Hotspot2.0 networks of different operators, configure a roaming consortium profile and add the organization identifiers (OIs) of the operators to the roaming consortium profile. In this way, after the user terminals connect to a network of an operator in the profile, they can roam to networks of the other operators while maintaining online.

Follow-up Procedure

Run the **roaming-consortium-oi** command to configure the roaming consortium OI in the roaming consortium profile.

Example

Create the roaming consortium profile **roaming-consortium-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] roaming-consortium-profile name roaming-consortium-profile1
[HUAWEI-wlan-ro-co-prof-roaming-consortium-profile1]
```


11.15.48 roaming-consortium-profile (Hotspot2.0 profile view)

Function

The **roaming-consortium-profile** command binds a roaming consortium profile to a Hotspot2.0 profile.

The **undo roaming-consortium-profile** command unbinds a roaming consortium profile from a Hotspot2.0 profile.

By default, no roaming consortium profile is bound to a Hotspot2.0 profile.

Format

roaming-consortium-profile *profile-name*

undo roaming-consortium-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a roaming consortium profile.	The roaming consortium profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services for networks. When user terminals connect to the networks, they can obtain OIs of the operators used for STA roaming, which helps them select desired networks. You can run the **roaming-consortium-profile** command to create a roaming consortium profile and the **roaming-consortium-oi** command in the roaming consortium profile view to configure operator OIs, and then bind the roaming consortium profile to a Hotspot2.0 profile to make the configuration take effect.

Example

Bind roaming consortium profile **roaming-consortium-profile1** to the Hotspot 2.0 profile **hotspot**.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] roaming-consortium-profile roaming-consortium-profile1
```

11.15.49 venue-name-profile

Function

The **venue-name-profile** command creates a venue name profile or displays the view of an existing venue name profile.

The **undo venue-name-profile** command deletes a venue name profile.

By default, no venue name profile is created.

Format

venue-name-profile name *profile-name*

undo venue-name-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a venue name profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all venue name profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, configure network parameters according to operator requirements. When connecting to networks, user terminals can obtain

the network parameters to select desired networks. The venue name describes physical locations of a network and is an optional parameter.

Follow-up Procedure

Run the **venue-name** command in the venue name profile view to configure the venue name. After creating a venue name profile, bind it to a Hotspot2.0 profile.

Example

Create the venue name profile **venue-name-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] venue-name-profile name venue-name-profile1
[HUAWEI-wlan-ve-na-prof-venue-name-profile1]
```

11.15.50 venue-name-profile (Hotspot2.0 profile view)

Function

The **venue-name-profile** command binds a venue name profile to a Hotspot2.0 profile.

The **undo venue-name-profile** command unbinds a venue name profile from a Hotspot2.0 profile.

By default, no venue name profile is bound to a Hotspot2.0 profile.

Format

venue-name-profile *profile-name*

undo venue-name-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a venue name profile.	The venue name profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services for networks. When connecting to the networks, user terminals can obtain location information of the networks from APs, which helps them to select desired networks. You can run the **venue-name-profile** command to create a venue name profile and the **venue-name** command in the venue name profile view to configure venue names, and then bind the venue name profile to a Hotspot2.0 profile to make the configuration take effect.

Example

Bind venue name profile **venue-name-profile1** to Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] venue-name-profile venue-name-profile1
```

11.15.51 venue-name

Function

The **venue-name** command configures a venue name for a Hotspot 2.0 network.

The **undo venue-name** command deletes the configured venue name.

By default, no venue name is configured.

Format

venue-name language-code *language-code* **name** *venue-name*

undo venue-name language-code *language-code* **name** *venue-name*

Parameters

Parameter	Description	Value
language-code *language-code*	Specifies the language type.	The value is a string of 2 to 3 characters. For the value of each language, see the definition in ISO639-2 *Codes for the Representation of Names of Languages*. For example, the value is **chi**, **zho**, or **zh** for Chinese, and **eng** for English.

Parameter	Description	Value
name *venue-name*	Specifies the venue name.	The value is a string of 1 to 64 case-sensitive characters. • English venue name: The value is a string of visible characters without question marks (?) and spaces. It cannot begin or end with double quotation marks (" "). • Non-English venue name: It cannot contain half-width question marks (?). To enter a non-English venue name, ensure that the remote login terminal supports the UTF-8 encoding format; otherwise, the name cannot be displayed.

Views

Venue name profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the command to configure venue names for Hotspot 2.0 networks to identify physical locations of the networks, which helps user terminals select desired networks. You can set the venue names in multiple languages for user groups of different languages.

Precautions

This command can be configured repeatedly. A maximum of 32 venue names can be configured in a venue name profile.

Example

Set the language to English and configure the venue name **CenterStation** in venue name profile **venue-name-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] venue-name-profile name venue-name-profile1
[HUAWEI-wlan-ve-na-prof-venue-name-profile1] venue-name language-code eng name CenterStation
```


11.15.52 venue-type

Function

The **venue-type** command configures the venue type of a Hotspot2.0 network.

The **undo venue-type** command deletes the configured venue type.

By default, no venue type information is configured for a Hotspot2.0 network.

Format

venue-type group-code *venue-group* **type-code** *type-code-value*

undo venue-type

Parameters

Parameter	Description	Value
group-code *venue-group*	Specifies the venue group type.	The value is an integer that ranges from 0 to 255. For meanings of different venue group values, see **7.3.1.34 Venue Info field** defined in IEEE Std 802.11u-2011.
type-code *type-code-value*	Specifies the venue subtype.	The value is an integer that ranges from 0 to 255. For meanings of different venue subtype values, see **7.3.1.34 Venue Info field** defined in IEEE Std 802.11u-2011.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple Hotspot2.0 networks are available, user terminals need to obtain information of each network to select the network to access. The venue type information is optional in a Hotspot2.0 profile. Beacon and Probe Response frames sent from Hotspot2.0-capable APs carry network parameter information, which helps user terminals to discover and select proper networks.

group-code and **type-code** determine the venue type and identify the network location. As predefined in the 802.11u protocol:

- If **group-code** is set to 2 (Business) and **type-code** to 3, the venue type indicates **Fire Station**.
- If **group-code** is set to 3 (Educational) and **type-code** to 3, the venue type indicates **University or College**.

Precautions

If the command is executed repeatedly, only the latest configuration takes effect.

Example

Set the venue type to **University or College** in Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] venue-type group-code 3 type-code 3
```

11.16 IoT AP Configuration Commands

11.16.1 Command Support

- WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.
- IoT cards are supported only by the following models:
  - AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 5760-51, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 8760-X1-PRO
  - AirEngine 5761-11W, AirEngine 5761-11WD, AirEngine 5761-12W, AirEngine 5761-21, AirEngine 5761S-11, AirEngine 5761S-11W, AirEngine 5761S-21, AirEngine 6761-21T, AirEngine 6761S-21T
  - AirEngine 5761-11, AirEngine 5761S-12, AirEngine 5761S-13, AirEngine 6761-21, AirEngine 6761S-21, AirEngine 6761-21E
  - AirEngine 5762-13W, AirEngine 5762-15HW, AirEngine 5762S-13W
  - AirEngine 5762-16W
  - AirEngine 8761-X1
  - AirEngine 5762-17W
  - AirEngine 8771-X1T

Only intrinsically safe APs (AirEngine 5761-11EI) support the baud rate configuration for communication between APs and IoT cards.

11.16.2 antenna-status

Function

The **antenna-status** command configures an IoT card to use the external or built-in antenna of an AP's IoT module.

The **undo antenna-status** command restores the default antenna selection policy for an IoT card.

By default, an IoT card is not configured to use the external or built-in antenna of an AP's IoT module.

Format

antenna-status { **external** | **internal** }

undo antenna-status

Parameters

Parameter	Description	Value
external	Configures an IoT card to use the external antenna of an AP's IoT module.	-
internal	Configures an IoT card to use the built-in antenna of an AP's IoT module.	-

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

By default, an IoT card uses the built-in 2.4 GHz antenna of an AP's IoT module for communication. You can install the external antenna as required and run the **antenna-status external** command to configure the IoT card to use the external antenna for communication.

NOTE

The external and built-in antennas cannot be used together in an IoT module. If there are multiple IoT cards, the cards must use the same type of antennas for communication. For configuration details, see Card 1.

When the **display ap-card all** or **display ap** *ap-id* **card** { **all** | *card-number* | **usb** } command is run to check information about an IoT card, whether the card uses the built-in or external antenna for communication is also displayed in the command output.

Example

Configure an IoT card to use the external antenna of an AP's IoT module.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name profile1
[HUAWEI-wlan-iot-prof-profile1] antenna-status external
```

11.16.3 baud-rate

Function

The **baud-rate** command configures the baud rate used by an AP to communicate with an IoT card.

The **undo baud-rate** command restores the default baud rate used by an AP to communicate with an IoT card.

By default, no baud rate is configured, and an AP can automatically adapt to the baud rate.

NOTE

This function is supported only by intrinsically safe APs (AirEngine 5761-11EI) that support communication with the uninterruptible power supply (UPS).

Format

baud-rate { **9600** | **19200** | **38400** | **57600** | **115200** | **921600** }

undo baud-rate

Parameters

Parameter	Description	Value
9600 | **19200** | **38400** | **57600** | **115200** | **921600**	Specifies the baud rate used by an AP to communicate with an IoT card.	-

Views

IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

APs with common cards can automatically adapt to the baud rate of an IoT card. However, for some cards, such as those with RS485 serial ports, APs cannot

automatically adapt to the card baud rate. In this case, run this command to set the baud rate to the same as that of the corresponding cards.

Example

Set the baud rate used by APs in an AP group to communicate with an IoT card to 9600 bit/s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] card 1
[HUAWEI-wlan-group-card-default/1]  baud-rate 9600
```

Set the baud rate used by an AP to communicate with an IoT card to 9600 bit/s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] card 1
[HUAWEI-wlan-card-0/1] baud-rate 9600
```

11.16.4 card connect-type

Function

The **card connect-type** command configures the connection type between IoT cards and APs.

The **undo card connect-type** command restores the default connection type between IoT cards and APs.

By default, IoT cards communicate with APs through serial interfaces.

Format

card connect-type { **ethernet** | **serial** | **container** }

undo card connect-type

Parameters

Parameter	Description	Value
ethernet	Configures IoT cards to communicate with APs through Ethernet interfaces.	-
serial	Configures IoT cards to communicate with APs through serial interfaces.	-
container	Configures IoT cards to communicate with a third-party server by loading the third-party container image.	-

Views

AP system profile view, IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When **serial** is configured for communication between IoT cards and APs, the communication rate does not exceed the maximum baud rate of serial interfaces, that is, 115200 bit/s. This connection type applies to scenarios with a light traffic volume. The connection type of **ethernet** applies to scenarios where electronic shelf labels (ESLs) are deployed.

Before using IoT cards of other vendors, contact the vendors to confirm the connection types supported by the cards.

Precautions

- The configurations in different views take effect in descending priority as follows: IoT card interface view of an AP > IoT card interface view of an AP group > AP system profile view.

Example

Configure IoT cards to communicate with APs through Ethernet interfaces.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ab
[HUAWEI-wlan-ap-system-prof-ab] card connect-type ethernet
```

11.16.5 config-agent permit ip-address

Function

The **config-agent permit ip-address** command configures trusted host computers.

The **undo config-agent permit ip-address** command deletes the configuration of trusted host computers.

By default, no trusted host computer is configured.

Format

config-agent permit ip-address *ip-address* { *net-mask* | *mask-len* }

undo config-agent permit ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a trusted host computer.	The value is in dotted decimal notation.
net-mask	Specifies the mask of the IP address of a trusted host computer.	The value is in dotted decimal notation.
mask-len	Specifies the mask length.	The value is an integer that ranges from 0 to 32.

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized devices from attacking an AP, you can configure trusted host computers. In this way, only hosts within the specified IP address range can communicate with the AP functioning as a server and send the AP the configuration to be delivered to the IoT card.

If no trusted host computer is configured, any host computers with reachable routes to the AP can communicate with the AP, which brings security risks to the AP.

Precautions

After the **type cas-edu** command is executed to set the card type to **cas-edu**, the **config-agent permit ip-address** command cannot be executed.

Example

Configure the IP address of a trusted host computer and its mask.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name wlan-iot
[HUAWEI-wlan-iot-prof-wlan-iot] config-agent permit ip-address 10.2.3.4 255.255.255.0
```


11.16.6 display ap card

Function

The **display ap card** command displays details about AP cards.

Format

display ap *ap-id* **card** { **all** | *card-number* | **usb** }

Parameters

Parameter	Description	Value
ap-id	Specifies an AP ID.	The AP ID must exist.
all	Specifies all AP cards.	-
card-number	Specifies an IoT card interface number.	The interface number must exist.
usb	Specifies the USB interface on an IoT card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display ap card** command to view details about AP cards.

Example

Display details about AP cards.

```
<HUAWEI> display ap 0 card all
Connected-status: The match status indicates that the card connection type matches
that on the device. Otherwise, mismatch is displayed. To modify the effective connection
type, run the card connect-type {serial|ethernet|container} command and restart the device.
--------------------------------------------------------------------------------
 Card                : 1
--------------------------------------------------------------------------------
 IOT card status     : absent
--------------------------------------------------------------------------------
 Card                : 2
--------------------------------------------------------------------------------
 IOT card status     : present
```



```
Card connect type       : Serial
Connected status        : mismatch

Physical connection type : PCIe
Support card information : YES
Protocol version        : 1
Wireless standard       : RFID
Frequency               : 433M
Vendor name             : ENJOYOR
Card type               : TOEAPV1.2
Hardware version        : VA
Firmware version        : 0.1.0.1
Card serial number      : 0000000000000001
Baud-rate               : 115200
Frame-version           : 1.0
Antenna status          : External
Card IP                 : 10.2.3.4
Card MAC                : 00e0-fc44-5566
Central frequency       : 2413MHz
Card bandwidth          : 2413MHz
Connect server status   : connected
Server name             : -
Subnet mask             : 16
Gateway address         : 10.2.3.5
--------------------------------------------------------------------------------
Card                    : 3
--------------------------------------------------------------------------------
IOT card status         : absent
--------------------------------------------------------------------------------
Card                    : usb
--------------------------------------------------------------------------------
USB status              : disable
IOT card status         : absent
--------------------------------------------------------------------------------
```

Table 11-303 Description of the **display ap card** command output

Item	Description
IOT card status	Card status. • present: A card is installed in the slot. • absent: No card is installed in the slot.
Card connect type	Connection type between an IoT card and the AP.
Physical connection type	Connection type between the IoT card and AP.
Connected status	Whether the actual connection type of an IoT card matches the current initialized connection type of the AP.
Support card information	Whether card information can be queried.
Protocol version	Protocol version. The current version number is 1.

Item	Description
Wireless standard	Wireless protocol supported by a card. The value is a 10-byte ASCII character set, for example, RFID, ANT, ZigBee, BT4.0, and Weightless.
Frequency	Card frequency. The value is an 8-byte ASCII character set, for example, 2.4G, 900M, 2.4/5G, or any value from 433M to 915M.
Vendor name	Vendor code. The value is an 8-byte ASCII character set, for example, ENJOYOR.
Card type	Card model. The value is a 12-byte ASCII character set, for example, TOEAPV1.2.
Hardware version	Hardware version of the card. The value is a 2-byte ASCII character set. The value is fixed in the following pattern: VA for the first version, VB for the second version, VC for the third version, and so on.
Firmware version	Firmware version of the card. The value is a 4-byte number, for example, 00.01.00.01.
Card serial number	Module ID of the card. The value is a 16-byte BCD character set.
Baud-rate	Baud rate for serial communication on an IoT card slot.
Frame-version	Frame format of an extension interface.
Antenna status	Whether an IoT card uses the built-in or external antenna. • External: external antenna • Internal: built-in antenna
Card IP	IP address of a card.
Card MAC	MAC address of an IoT card.
Central frequency	Center frequency of an IoT card.
Card bandwidth	Bandwidth of an IoT card.
Connect server status	Connection status between an IoT card and the server.

Item	Description
Server name	Name of the server connected to an IoT card.
Subnet mask	Subnet mask length.
Gateway address	Gateway address.
USB status	Actual working status of the USB function on an AP.

11.16.7 display ap-card statistics

Function

The **display ap-card statistics** command displays statistics on the packets received and sent by cards on APs.

Format

display ap-card statistics { **all** | **ap-id** *ap-id* [**card** { *card-number* | **usb** }] }

Parameters

Parameter	Description	Value
all	Specifies cards on all APs.	-
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-number*	Specifies an IoT card interface number.	The interface number must exist.
usb	Specifies the USB interface on an IoT card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check statistics on the packets received and sent by cards on APs. Only statistics about IoT cards with the serial connection type can be displayed.

Example

Display statistics on the packets received and sent by cards on all APs.

```
<HUAWEI> display ap-card statistics all
-------------------------------------------------------------------------------------------------
AP ID  Card-number  RX-packets  TX-packets  RX-bytes  TX-bytes
-------------------------------------------------------------------------------------------------
0      1           1           2           100       200
-------------------------------------------------------------------------------------------------
Total: 1
```

Display statistics on the packets received and sent by cards on AP 0.

```
<HUAWEI> display ap-card statistics ap-id 0
-------------------------------------------------------------------------------------------------
AP ID  Card-number  Card-status  RX-packets  TX-packets  RX-bytes  TX-bytes
-------------------------------------------------------------------------------------------------
0      1           present      1           2           100       200
0      2           absent       2           1           89        14
0      3           absent       0           0           0         0
0      usb          absent       0           0           0         0
-------------------------------------------------------------------------------------------------
Total: 4
```

Table 11-304 Description of the **display ap-card statistics** command output

Item	Description
AP ID	AP ID.
Card-number	Card number.
Card-status	Whether a card is installed in the slot. • absent: No card is installed in the slot. • present: A card is installed in the slot.
RX-packets	Number of packets sent to a card.
TX-packets	Number of packets received from a card.
RX-bytes	Number of bytes sent to a card.
TX-bytes	Number of bytes received from a card.

11.16.8 display ap-card all

Function

The **display ap-card all** command displays brief information about cards on all the APs.

Format

display ap-card all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To query brief information about cards on all the APs, run the **display ap-card all** command.

Precautions

No result is displayed if a card does not support query.

Example

Display brief information about cards on all the APs.

```
<HUAWEI> display ap-card all
Connected-status: The match status indicates that the card connection type matches
that on the device. Otherwise, mismatch is displayed. To modify the effective connection
type, run the card connect-type {serial|ethernet|container} command.
Frame-version: Frame format on extended interfaces.
--------------------------------------------------------------------------------------------------------------------------------
-------
---------------------------
AP ID  Card-number  Wireless-standard  Vendor-name  Card-type     Card-connect-type  Connected-status
Antenna-status  Baud-rate  Fr
ame-version  Serial-number
--------------------------------------------------------------------------------------------------------------------------------
-------
---------------------------
0      1            RFID               ENJOYOR      TOEAPV1.2     ethernet(up)       match              External
9600       2.
0            0000000000000001
--------------------------------------------------------------------------------------------------------------------------------
-------
---------------------------
Total: 1
```

Table 11-305 Description of the **display ap-card all** command output

Item	Description
AP ID	AP ID.
Card-number	Card ID.

Item	Description
Wireless-standard	Wireless protocol supported by a card. The value is a 10-byte ASCII character set, for example, RFID, ANT, ZigBee, BT4.0, and Weightless.
Vendor-name	Vendor code. The value is an 8-byte ASCII character set, for example, ENJOYOR.
Card-type	Card model. The value is a 12-byte ASCII character set, for example, TOEAPV1.2.
Card-connect-type	Connection type between an IoT card and the AP.
Connected-status	Whether the actual connection type of an IoT card matches the current initialized connection type of the AP.
Antenna-status	Whether an IoT card uses the built-in or external antenna. • External: external antenna • Internal: built-in antenna
Baud-rate	Baud rate used for communication between the card and AP.
Frame-version	Frame format of an extension interface.
Serial-number	Module ID of a card. The value is a 16-byte BCD character set.

11.16.9 display iot-card iot-command-result

Function

The **display iot-card iot-command-result** command displays the execution results of commands transparently transmitted to IoT cards.

Format

display iot-card iot-command-result all

display iot-card iot-command-result ap ap-id *ap-id* **card** { *card-id* | **usb** }

Parameters

Parameter	Description	Value
all	Displays command execution results on all cards of all APs.	-
ap ap-id *ap-id*	Displays command execution results on cards of the AP with a specified ID.	The AP ID must exist.
card *card-id*	Displays command execution records on the card with a specified ID.	The value is an integer that ranges from 1 to 3.
card usb	Displays command execution results on USB cards.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a command is transparently transmitted to a card, you can run the **display iot-card iot-command-result** command to check the command execution result on the card.

Precautions

Example

Display execution results of commands transparently transmitted to all IoT cards.

```
<HUAWEI> display iot-card iot-command-result all
Ap information:
Total  :    [7]
Waiting:    [1]
Success:    [1]
Fail   :    [5]
-------------------------------------------------------------------------------------------------------------------
AP-ID Card Time                Command  Transparent transmission result
Card Response
-------------------------------------------------------------------------------------------------------------------
13    1    2019.10.10 16:14:46  status   Fail(Time Out)
13    1    2019.10.10 16:31:24  status   Success
++++++++++++++++++++++++++++++++
- Network:
DHCP:           BOUND
IP:             10.10.10.54
Netmask:        255.255.255.0
```



```
Gateway:        10.10.10.1
Nameserver:     0.0.0.0
Nameserver2:    0.0.0.0
- ESL SCD:
ID:             42002

++++++++++++++++++++++++++++++++
11    1    2019.10.10 16:14:46  status   Fail(Card is not installed)
12    1    2019.10.10 16:14:46  status   Fail(Card is busy)
14    1    2019.10.10 16:14:46  status   Fail(Other reason)
15    1    2019.10.10 16:14:46  status   Fail(Time out)
15    1    2019.10.10 16:14:46  status   Waiting
--------------------------------------------------------------------------------------------------------------------------------
Total: 7
```

Table 11-306 Description of the **display iot-card iot-command-result all** command output

Item	Description
Total	Total number of command execution results.
Waiting	Number of command execution results that a card is waiting for from the AP.
Success	Number of commands that have been successfully executed.
Fail	Number of commands that fail to be executed.
AP-ID	ID of the AP where a card resides.
Card	Card ID.
Time	Time when the device transparently transmits a command to a card.
Command	Content of a command transparently transmitted to a card.

Item	Description
Transparent transmission result	Execution result of a command on a card: • Success: The command has been successfully executed. • Waiting: The card is waiting for a response from the AP. • Fail: The command fails to be transmitted to the card. The failure reasons are as follows: – Card does not support this command: The card does not support this command. – Card is not installed: The card is not properly installed. – Time Out: The response of the card times out. Check the version of the card. If the card version does not support transparent transmission of commands, the command execution times out. – Card is busy: The card is executing another command. – Other reason: A system error occurs.
Card Response	Response of a card. The response is defined by the card vendor. For details, contact the card vendor.

11.16.10 display iot-profile

Function

The **display iot-profile** command displays the IoT profile configuration.

Format

display iot-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an IoT profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Specifies all IoT profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view the IoT profile configuration.

Example

Display the configuration of all IoT profiles.

```
<HUAWEI> display iot-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
1                               0
profile1                          0
wlan-IoT                          1
--------------------------------------------------------------------------------
Total:3
```

Table 11-307 Description of the **display iot-profile all** command output

Item	Description
Profile name	Name of an IoT profile.
Reference	Number of times an IoT profile is referenced.

Display the configuration of the IoT profile **wlan-IoT** .

```
<HUAWEI> display iot-profile name wlan-IoT
-------------------------------------------------------------------------------
Type                          : common
Agent permit IP address       : 10.23.102.253
Agent permit net-mask         : 255.255.255.0
Management server IP address  : 10.23.102.254
Management server port        : 3000
ExtManagement server IP address  : -
ExtManagement server port     : -
Share key                     : ******
Antenna status                : -
-------------------------------------------------------------------------------
```

Table 11-308 Description of the **display iot-profile name wlan-IoT** command output

Item	Description
Type	Card type. To configure this parameter, run the **type (IoT profile view)** command.
Agent permit IP address	IP address of a trusted host computer. To configure this parameter, run the **config-agent permit ip-address** command.
Agent permit net-mask	Mask of the IP address of a trusted host computer. To configure this parameter, run the **config-agent permit ip-address** command.
Management server IP address	IP address of the host computer. To configure this parameter, run the **management-server** command.
Management server port	Port number of the host computer. To configure this parameter, run the **management-server** command.
ExtManagement server IP address	IP address of the host computer on the extended channel. To configure this parameter, run the **management-server** command.
ExtManagement server port	Port number of the host computer on the extended channel. To configure this parameter, run the **management-server** command.
Share key	Shared key. To configure this parameter, run the **share-key** command.

Item	Description
Antenna status	Whether an IoT card uses the built-in or external antenna. • External: external antenna • Internal: built-in antenna

11.16.11 display references iot-profile

Function

The **display references iot-profile** command displays reference information about an IoT profile.

Format

display references iot-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an IoT profile.	The IoT profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view reference information about an IoT profile.

Example

Display reference information about the IoT profile **wlan-IoT**.

```
<HUAWEI> display references iot-profile name wlan-IoT
------------------------------------------------------------------------------
Reference type     Reference name                Reference card
------------------------------------------------------------------------------
AP group           default                       Card-1
------------------------------------------------------------------------------
Total:1
```


Table 11-309 Description of the **display references iot-profile name wlan-IoT** command output

Item	Description
Reference type	Type of the object to which the IoT profile is bound.
Reference name	Name of the object to which the IoT profile is bound.
Reference card	Card to which the IoT profile is bound.

11.16.12 card

Function

The **card** command displays the IoT card interface view.

Format

card { *card-number* | **usb** }

Parameters

Parameter	Description	Value
card-number	Specifies an IoT card interface number.	The value is an integer that ranges from 1 to 3.
usb	Specifies the USB interface for an IoT card.	-

Views

AP group view, AP specific view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the communication parameters are configured between an AP and an IoT card, and between an AP and a host computer, you need to bind corresponding configuration profiles in the IoT card interface view to make the parameters take effect.

Prerequisites

The USB function of the AP has been enabled using the **usb enable** command.

Precautions

IoT cards of the cas-edu type do not support the USB interface.

Example

Display the IoT card interface view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] card 1
[HUAWEI-wlan-group-card-default/1]
```

11.16.13 iconnect enable

Function

The **iconnect enable** command enables the iConnect function on an AP so that the AP releases an iConnect SSID.

The **undo iconnect enable** command disables the iConnect function.

By default, the iConnect function is disabled.

Format

iconnect enable

undo iconnect enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the iConnect function is enabled on an AP, the AP releases an iConnect SSID, through which IoT terminals can access the network. This implements plug-and-play of IoT terminals and enables the terminals to automatically load digital certificates.

Precautions

In the Navi AC scenario, an SSID cannot be configured as an iConnect SSID.

Example

Enable the iConnect function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] iconnect enable
```

11.16.14 iot-card reboot

Function

The **iot-card reboot** command resets an IoT card of an AP.

Format

iot-card reboot ap ap-id *ap-id* **card** { *card-id* | **usb** }

Parameters

Parameter	Description	Value
ap ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card-id	Specifies the IoT card interface number.	The value is an integer that ranges from 1 to 3.
usb	Specifies the USB interface of an IoT card.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

The **iot-card reboot** command resets an IoT card of an AP.

Example

Reset an IoT card on the USB interface of the AP with ID 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-card reboot ap ap-id 0 card usb
```


11.16.15 iot-card reset-factory-configuration

Function

The **iot-card reset-factory-configuration** command restores factory defaults of an IoT card.

Format

iot-card reset-factory-configuration ap ap-id *ap-id* **card** *card-id*

Parameters

Parameter	Description	Value
ap ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-id*	Specifies the ID of an IoT card.	The IoT card ID must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an IoT card cannot communicate with the AP due to an error in IoT card parameter settings, you can run this command to restore factory defaults of the IoT card.

Example

Restore factory defaults of an IoT card.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-card reset-factory-configuration ap ap-id 1 card 1
```

11.16.16 iot-card reset-network-configuration

Function

The **iot-card reset-network-configuration** command resets network parameters of an IoT card.

Format

iot-card reset-network-configuration ap ap-id *ap-id* **card** { *card-id* | **usb** }

Parameters

Parameter	Description	Value
ap ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-id*	Specifies the ID of an IoT card.	The IoT card ID must exist.
card usb	Specifies an IoT card of the USB type.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An IoT card involves network parameters for communicating with a host computer (such as the card IP address, server IP address, and DNS address) and air interface parameters in a wireless environment. In most cases, when the wireless environment becomes stable, air interface parameters remain unchanged. When the wired environment changes, you can only run the **iot-card reset-network-configuration** command to reset network parameters of the IoT card. During this process, the air interface parameters remain unchanged.

This command is supported only by **Ethernet port cards**.

Example

Reset network parameters of an IoT card.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-card reset-network-configuration ap ap-id 1 card 1
```

11.16.17 iot-card switch-firmware

Function

The **iot-card switch-firmware** command switches the active and standby partitions of an IoT card.

Format

iot-card switch-firmware ap ap-id *ap-id* **card** *card-id*

Parameters

Parameter	Description	Value
ap ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-id*	Specifies the ID of an IoT card.	The IoT card ID must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Upon a fault on the current partition of an IoT card, you can run this command to switch to the other partition.

Example

Switch the active and standby partitions of an IoT card.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-card switch-firmware ap ap-id 1 card 1
```

11.16.18 iot-profile (WLAN view)

Function

The **iot-profile** command creates an IoT profile and displays the IoT profile view.

The **undo iot-profile** command deletes an IoT profile.

By default, no IoT profile is created.

Format

iot-profile name *profile-name*

undo iot-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an IoT profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Specifies all IoT profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP functions as a server or client to communicate with the host computer in bi-directional mode. When the AP reports data to the host computer, the AP functions as a client and the host computer functions as a server. When the AP receives data from the host computer, the AP functions as a server and the host computer functions as a client.

Example

Create IoT profile **profile1** and display the IoT profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name profile1
[HUAWEI-wlan-iot-prof-profile1]
```

11.16.19 iot-profile (IoT card interface view)

Function

The **iot-profile** command binds an IoT profile to an IoT card interface, and configures the local port number mapping the IoT card interface.

The **undo iot-profile** command unbinds an IoT profile from an IoT card interface.

By default, no IoT profile is bound to an IoT card interface.

Format

iot-profile *profile-name* **config-agent** { **tcp** | **udp** } [**port** *port*] [**ext-port** *ext-port*]

undo iot-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an IoT profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
tcp	Configures the AP to communicate with the host computer using TCP.	-
udp	Configures the AP to communicate with the host computer using UDP.	-
port *port*	Specifies the source port for the first channel.	The value is an integer that ranges from 1025 to 55535. By default, the port number is a random port number in the range of 49152 to 65535. **NOTE** A port number within the range from 50200 to 50202 is recommended. If another port number is used, a port conflict may occur and an alarm is generated.

Parameter	Description	Value
ext-port *ext-port*	Specifies the source port for the extended channel.	The value is an integer that ranges from 1025 to 55535. By default, the port number is a random port number in the range of 49152 to 65535. **NOTE** A port number within the range from 50200 to 50202 is recommended. If another port number is used, a port conflict may occur and an alarm is generated.

Views

IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to bind an IoT profile, configure the communication protocol between the AP and host computer, and configure the source port number for the IoT card interface.

Example

Bind IoT profile **profile1** and set the local UDP port number to 50200.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] card 1
[HUAWEI-wlan-group-card-default/1] iot-profile profile1 config-agent udp port 50200
```

11.16.20 management-server

Function

The **management-server** command configures a host computer.

The **undo management-server** command deletes the host computer configuration.

By default, no host computer is configured.

Format

management-server { **domain** *domain-name* | **server-ip** *server-ip* } **server-port** *server-port-num* [**ext-channel**]

undo management-server { **domain** *domain-name* | **server-ip** *server-ip* } [**server-port** *server-port-num*] [**ext-channel**]

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name of a host computer.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, and underscores (_) or dots (.).
server-ip *server-ip*	Specifies the IP address of a host computer.	The value is in dotted decimal notation.
server-port *server-port-num*	Specifies the port number of a host computer.	The value is an integer that ranges from 1 to 65535.
ext-channel	Specifies an extension channel.	-

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP functions as a server or client to communicate with a host computer in bi-directional mode. When the AP reports data (Huawei APs only transparently transmit data to the host computer, and do not parse or collect data) to the host computer, the AP functions as a client and the host computer functions as a

server. When the AP receives data from the host computer, the AP functions as a server and the host computer functions as a client. The domain name/IP address and one port of at least one host computer must be configured. Otherwise, serial data reported by the AP will be discarded.

Precautions

You can configure multiple host computers. An IoT card of the **common** type supports a maximum of four host computers. After four host computers have been configured, you need to delete a host computer before adding a new host computer. Host computers can only be deleted or added, but cannot be modified. An IoT card of the **cas-edu** type supports only one host computer.

When a ZigBee card is used, information about two host computers must be configured. The channel of the second host computer is an extension channel specified by the **ext-channel** parameter. Only one extension channel can be configured. The two channels cannot be configured with the same port number and IP address, or the same port number and domain name.

When multiple host computers are configured, the device automatically selects one available host computer for link establishment rather than establish links with multiple host computers.

Example

Configure an IP address and a port number for a host computer.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name profile1
[HUAWEI-wlan-iot-prof-profile1] management-server server-ip 10.1.1.2 server-port 3000
```

11.16.21 reset ap-card statistics

Function

The **reset ap-card statistics** command clears statistics on the packets received and sent by cards on APs.

Format

reset ap-card statistics { **all** | **ap-id** *ap-id* [**card** { *card-number* | **usb** }] }

Parameters

Parameter	Description	Value
all	Specifies cards on all APs.	-
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-number*	Specifies an IoT card interface number.	The interface number must exist.

Parameter	Description	Value
usb	Specifies the USB interface on an IoT card.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to clear statistics on the packets received and sent by cards on APs. Only statistics about IoT cards with the serial connection type can be cleared.

Precautions

The statistics cannot be restored after being cleared.

Example

Clear statistics on the packets received and sent by cards on all APs.

```
<HUAWEI> reset ap-card statistics all
```

11.16.22 share-key

Function

The **share-key** command configures a shared key.

The **undo share-key** command deletes a shared key.

By default, no shared key is configured.

Format

share-key *key-value*

undo share-key

Parameters

Parameter	Description	Value
key-value	Specifies a shared key.	The value is a string of characters. • The key in plaintext contains 6 to 32 characters. • The key in ciphertext contains 48 or 68 characters. **NOTE** To ensure security, a shared key must be a combination of at least two of the following: digits, lowercase letters, uppercase letters, and special characters.

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure a shared key to improve data communication security and ensure completeness of packets exchanged between an AP and host computers. The shared key must be the same on the AP and host computers.

Precautions

After the **type cas-edu** command is executed to set the card type to **cas-edu**, the **share-key** command cannot be executed.

Example

Set the shared key to **aabb0011@11**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name profile1
[HUAWEI-wlan-iot-prof-profile1] share-key aabb0011@11
```


11.16.23 type (IoT profile view)

Function

The **type** command sets the type of an IoT card.

The **undo type** command restores the default IoT card type.

The default type of an IoT card is **common**.

Format

type { **cas-edu** | **common** }

undo type

Parameters

Parameter	Description	Value
cas-edu	Indicates an IoT card that complies with IoT standards of the China Academy of Science.	-
common	Indicates an IoT card that complies with Huawei's IoT standards.	-

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an interconnection with the education system solution of the China Academy of Science, set the IoT card type to **cas-edu**. In other scenarios, set the IoT card type to **common**.

Precautions

After the IoT card type is modified in an IoT profile, other parameters in this IoT profile will restore to the default values.

If the **iot-profile (IoT card interface view)** command has been executed to bind an IoT profile, the IoT card type cannot be modified. The IoT card type can be modified only after the IoT profile is unbound.

After the **type cas-edu** command is executed to set the card type to **cas-edu**, the **config-agent permit ip-address** and **share-key** commands cannot be executed.

Example

Set the IoT card type to **cas-edu**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name wlan-iot
[HUAWEI-wlan-iot-prof-wlan-iot] type cas-edu
Warning: After the card type is modified, related configuration items in the profile are cleared. Continue?
[Y/N]:y
```

11.16.24 wired-port-profile (IoT card interface view)

Function

The **wired-port-profile** command binds a specified AP wired port profile to an IoT card.

The **undo wired-port-profile** command unbinds the AP wired port profile from an IoT card.

By default, no AP wired port profile is bound to an IoT card.

Format

wired-port-profile *profile-name*

undo wired-port-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port profile.	The AP wired port profile must exist.

Views

IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an IoT card communicates with an AP through an Ethernet interface, to configure this Ethernet interface, you can set parameters in an AP wired port profile and bind it to the IoT card.

Prerequisites

The IoT card has been configured to communicate with the AP through an Ethernet interface using the **card connect-type ethernet** command.

Example

Bind the AP wired port profile **wired-port1** to an IoT card.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] quit
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] card 1
[HUAWEI-wlan-group-card-default/1] wired-port-profile wired-port1
```

11.17 WLAN Traffic Optimization Commands

11.17.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.17.2 display wlan igmp-snooping vap-cac

Function

The **display wlan igmp-snooping vap-cac** command displays the multicast CAC configuration and statistics on a VAP.

Format

display wlan igmp-snooping vap-cac { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the multicast CAC configuration and statistics on a VAP, including the bandwidth and user statistics.

Example

Display the multicast CAC configuration and statistics on VAPs of the AP with ID 0.

```
<HUAWEI> display wlan igmp-snooping vap-cac ap-id 0
Info: This operation may take a few seconds, please wait.done.
Rf            : Radio ID                  WID             : WLAN ID
CurBw         : Current bandwidth(kbps)   MaxBw           : Max bandwidth(kbps)
CurUser       : Current user number       MaxUser         : Max user number
BwUtilization : Bandwidth utilization     UserUtilization : User utilization
--------------------------------------------------------------------------------
Rf  WID  CurBw/MaxBw       BwUtilization  CurUser/MaxUser  UserUtilization
--------------------------------------------------------------------------------
0   1    0/11              0%             0/6              0%
--------------------------------------------------------------------------------
Total: 1
```

Table 11-310 Description of the **display wlan igmp-snooping vap-cac** command output

Item	Description
Rf	Radio ID.
WID	WLAN ID.
CurBw/MaxBw	Current multicast bandwidth/ Maximum multicast bandwidth of a VAP.
BwUtilization	Multicast bandwidth utilization.
CurUser/MaxUser	Current number of multicast users/ Maximum number of multicast users on a VAP.
UserUtilization	Multicast user utilization.

11.17.3 igmp-snooping group-bandwidth (AP system profile view)

Function

The **igmp-snooping group-bandwidth** command configures the bandwidth of global multicast groups on an AP.

The **undo igmp-snooping group-bandwidth** command deletes the bandwidth of global multicast groups on an AP.

By default, the bandwidth of global multicast groups is not configured on an AP.

Format

igmp-snooping group-bandwidth start-group-address *start-group-address* **end-group-address** *end-group-address* **bandwidth** *bandwidth-value*

undo igmp-snooping group-bandwidth start-group-address *start-group-address* **end-group-address** *end-group-address*

Parameters

Parameter	Description	Value
start-group-address *start-group-address*	Specifies the start multicast group address.	The value is in dotted decimal notation.
end-group-address *end-group-address*	Specifies the end multicast group address.	The value is in dotted decimal notation.
bandwidth *bandwidth-value*	Specifies the bandwidth of multicast groups.	The value is an integer that ranges from 1 to 100000, in kbps.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the bandwidth of multicast groups in an AP system profile according to the actual bandwidth of a multicast program. This configuration takes effect for the APs or AP groups to which this AP system profile is bound. When users request to order this multicast program, the collects statistics on the current multicast bandwidth of the VAP according to the configured bandwidth of global multicast groups, and compares the current bandwidth with the configured maximum bandwidth to determine whether to allow users to order this multicast program.

Precautions

You can configure the bandwidth for a maximum of 32 multicast group address segments. Addresses in one address segment must be different from those in another address segment. The configured address segments must contain valid multicast program addresses.

Example

Set the bandwidth to 100 kbps for multicast group address segment from 224.0.1.0 to 224.255.255.255.


```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] igmp-snooping group-bandwidth start-group-address
224.0.1.0 end-group-address 224.255.255.255 bandwidth 100
```

11.17.4 igmp-snooping max-bandwidth (traffic profile view)

Function

The **igmp-snooping max-bandwidth** command configures the maximum multicast bandwidth for a VAP.

The **undo igmp-snooping max-bandwidth** command deletes the maximum multicast bandwidth of a VAP.

By default, the maximum multicast bandwidth is not configured for a VAP.

Format

igmp-snooping max-bandwidth *max-bandwidth*

undo igmp-snooping max-bandwidth

Parameters

Parameter	Description	Value
max-bandwidth	Specifies the maximum multicast bandwidth of a VAP.	The value is an integer that ranges from 1 to 10000000, in kbit/s.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum multicast bandwidth is configured for a VAP in a traffic profile to limit the multicast traffic forwarding capacity of the VAP to which this traffic profile is bound. When the available multicast bandwidth of a VAP is insufficient, new users are prevented from joining multicast groups.

Precautions

After configuring the maximum multicast bandwidth for a VAP, run the **igmp-snooping group-bandwidth (AP system profile view)** command to configure the bandwidth of global multicast groups on the AP.

If the specified maximum multicast bandwidth is smaller than the actual volume of running multicast services, user services may be interrupted.

Example

Set the maximum multicast bandwidth to 500 kbit/s in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping max-bandwidth 500
```

11.17.5 igmp-snooping max-user (traffic profile view)

Function

The **igmp-snooping max-user** command configures the maximum number of multicast group memberships for a VAP.

The **undo igmp-snooping max-user** command deletes the maximum number of multicast group memberships for a VAP.

By default, the maximum number of multicast group memberships is not configured for a VAP.

Format

igmp-snooping max-user *max-user*

undo igmp-snooping max-user

Parameters

Parameter	Description	Value
max-user	Specifies the maximum number of multicast group memberships on a VAP.	The value is an integer that ranges from 1 to 1000.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum number of multicast group memberships on a VAP is configured in a traffic profile to limit access of multicast users on the VAP to which this traffic

profile is bound. When the number of multicast group memberships on a VAP reaches the maximum value, new users are prevented from joining multicast groups.

Precautions

If the specified maximum number of multicast group memberships is smaller than the actual number of access multicast users, user services may be interrupted.

Example

Set the maximum number of multicast group memberships to 10 on the VAP to which traffic profile **p1** is bound.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping max-user 10
```

11.17.6 igmp-snooping enable (traffic profile view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a traffic profile.

The **undo igmp-snooping enable** command disables IGMP snooping in a traffic profile.

By default, IGMP snooping is disabled in a traffic profile.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP snooping is a basic Layer 2 multicast function that forwards and controls multicast traffic at the data link layer. IGMP snooping runs on a Layer 2 device and analyzes IGMP messages exchanged between a Layer 3 device and hosts to set up and maintain a Layer 2 multicast forwarding table. The Layer 2 device forwards multicast packets based on the Layer 2 multicast forwarding table.

After you disable IGMP snooping in a traffic profile using the **undo igmp-snooping enable** command, all IGMP snooping configurations in the traffic profile are deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping again, all IGMP snooping configurations are restored to the default settings on the device.

Prerequisites

The traffic profile has been created using the **traffic-profile (WLAN view)** command.

This command is used to enable Layer 2 multicast services. To ensure multicast service experience, you are advised to run the **traffic-optimize broadcast-suppression other-multicast disable** command in the AP system profile view to disable rate limiting for multicast packets. In addition, run the **anti-attack flood igmp disable** and **anti-attack flood other-multicast disable** commands in the VAP profile view to disable floor attack defense for multicast packets.

When multicast services are enabled, the multicast services may be affected if rate limiting for multicast packets is enabled on an AP. In this case, you are advised to run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command to adjust the rate limit threshold for multicast packets.

When multicast services are enabled, the multicast services may be affected if flood attack defense is disabled in the VAP profile view. In this case, you are advised to run the **anti-attack flood { igmp | other-multicast } sta-rate-threshold** *sta-rate-threshold* command to adjust the flood attack threshold for multicast packets.

Example

Enable IGMP snooping in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping enable
```

11.17.7 igmp-snooping report-suppress (Traffic profile view)

Function

The **igmp-snooping report-suppress** command enables suppression of IGMP Report and Leave message in a traffic profile.

The **undo igmp-snooping report-suppress** command cancels configuration of IGMP Report and Leave message suppression in a traffic profile.

By default, IGMP Report and Leave message suppression is disabled in a traffic profile.

Format

igmp-snooping report-suppress

undo igmp-snooping report-suppress

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an IGMP Membership Report message (Report or Leave message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an IGMP General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages in the same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.
- A host running IGMPv2 or IGMPv3 sends a Leave message when leaving a multicast group. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Leave messages from the member hosts.

After this function is configured, a Layer 2 device forwards only one IGMP Membership Report message to the upstream device in the following scenarios: When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device then creates or maintains the matching forwarding entry based on the Report message. When the last member of a group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry. This reduces the number of IGMP messages on the network.

Prerequisites

IGMP snooping has been enabled using the **igmp-snooping enable (traffic profile view)** command.

Example

Enable suppression of IGMP Report and Leave messages in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping enable
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping report-suppress
```


11.17.8 mld-snooping enable (traffic profile view)

Function

The **mld-snooping enable** command enables MLD snooping in a traffic profile.

The **undo mld-snooping enable** command disables MLD snooping in a traffic profile.

By default, MLD snooping is disabled in a traffic profile.

Format

mld-snooping enable

undo mld-snooping enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **mld-snooping enable** command to enable MLD snooping in a traffic profile.

After you disable MLD snooping in a traffic profile using the **undo mld-snooping enable** command, all MLD snooping configurations in the traffic profile are deleted. When you run the **mld-snooping enable** command to enable MLD snooping again, all MLD snooping configurations are restored to the default settings in the traffic profile.

Prerequisites

A traffic profile has been created.

Before enabling MLD snooping in a traffic profile, run the **sta-ipv6-service enable** commands to enable the function of processing STA IPv6 services in the WLAN view.

Example

Enable MLD snooping in traffic profile **p1**.

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



```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] mld-snooping enable
```

11.17.9 service-guarantee

Function

The **service-guarantee** command configures the service guarantee mode.

The **undo service-guarantee** command restores the default service guarantee mode.

The default service guarantee mode is performance-first.

Format

service-guarantee { **performance-first** | **reliability-first** }

undo service-guarantee

Parameters

Parameter	Description	Value
performance-first	Sets the service guarantee mode to performance-first.	-
reliability-first	The service guarantee mode is set to reliability-first.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP is connected to a VR device, retransmission of lost packets has a great impact on user experience. Therefore, you can set the service guarantee mode to reliability first. That is, when the VR throughput requirement is met, the air interface rate can be lowered properly to reduce jitter and delay caused by packet loss and retransmission, improving user experience. It is recommended that the service assurance mode be set to reliability first in VR gaming scenarios and to performance first in VR video scenarios.

Precautions

Changing the service guarantee mode will interrupt services of associated STAs.

Traffic optimization in VR scenarios is supported only by APs in compliance with 802.11ac Wave 2, 802.11ax and later standards.

Example

Set the service guarantee mode to reliability-first.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] service-guarantee reliability-first
```

11.17.10 traffic-optimize arp-proxy enable

Function

The **traffic-optimize arp-proxy enable** command enables ARP proxy on the device.

The **undo traffic-optimize arp-proxy enable** command disables ARP proxy on the device.

By default, ARP proxy is disabled.

Format

traffic-optimize arp-proxy enable

undo traffic-optimize arp-proxy enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an ARP Request packet is sent from a user or the network to another user, the AC or AP enabled with ARP proxy can reply to this packet. Compared with the function of converting ARP multicast packets to ARP unicast packets, ARP proxy can reduce the number of times a sleeping terminal is awakened to save power.

Precautions

The ARP proxy function is not available for roaming users.

Example

Enable ARP proxy on the device in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize arp-proxy enable
```

11.17.11 traffic-optimize bcmc deny all

Function

The **traffic-optimize bcmc deny all** command configures the air interface to deny downlink broadcast and multicast packets.

The **undo traffic-optimize bcmc deny all** command cancels the configuration of denying downlink broadcast and multicast packets on the air interface.

By default, the air interface does not deny downlink broadcast or multicast packets.

Format

traffic-optimize bcmc deny all [**except mdns**]

undo traffic-optimize bcmc deny all

Parameters

Parameter	Description	Value
except mdns	If this parameter is configured, mDNS packets are allowed to pass through when the air interface is configured to deny broadcast and multicast packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IP network, the ARP, ND, and DHCP protocols are the basic network protocols and serve as the basis for packet forwarding on the entire network.

Broadcast or multicast packets of protocols other than the ARP, ND, and DHCP protocols are optional on the IP network. When no services rely on transmission of these broadcast or multicast packets on the network, you can run the command to configure the air interface to deny all broadcast and multicast packets to improve the air interface performance.

Precautions

Before using the **traffic-optimize bcmc deny all** command to configure the air interface to deny downlink broadcast and multicast packets on the AP, run the **undo learn-client-address { ipv4 | ipv6 } disable** command to enable STA address learning and the **traffic-optimize bcmc unicast-send** { **arp** | **nd** | **dhcp** | **mdns** } * command to configure the broadcast/multicast-to-unicast conversion function on the air interface. Otherwise, the ARP, ND, and DHCP packets may fail to be forwarded.

Example

Configure the air interface to deny downstream broadcast and multicast packets in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize bcmc deny all
```

11.17.12 traffic-optimize bcmc unicast-send

Function

The **traffic-optimize bcmc unicast-send** { **arp** | **nd** | **dhcp** | **mdns** }* command configures the broadcast/multicast-to-unicast conversion function on the air interface.

The **undo traffic-optimize bcmc unicast-send** { **arp** | **nd** | **dhcp** | **mdns** }* command cancels the configuration of the broadcast/multicast-to-unicast conversion function on the air interface.

The **undo traffic-optimize bcmc unicast-send** command restores the default configuration.

By default, the broadcast/multicast-to-unicast conversion function is enabled for ARP, ND, and DHCP packets but disabled for mDNS packets on the air interface.

Format

traffic-optimize bcmc unicast-send { **arp** | **nd** | **dhcp** | **mdns** }*

undo traffic-optimize bcmc unicast-send { **arp** | **nd** | **dhcp** | **mdns** }*

undo traffic-optimize bcmc unicast-send

Parameters

Parameter	Description	Value
arp	Specifies ARP packets.	-
nd	Specifies ND packets.	-
dhcp	Specifies DHCP packets.	-
mdns	Specifies mDNS packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an air interface sends a large number of broadcast or multicast packets when being busy, the performance of the air interface will drop. To prevent this situation, you can configure the broadcast/multicast-to-unicast conversion function to reduce the number of broadcast or multicast packets transmitted on the air interface. This improves air interface performance at the price of increased CPU usage.

Prerequisites

The **undo learn-client-address { ipv4 | ipv6 } disable** command has been executed to enable STA address learning.

Example

Configure the broadcast/multicast-to-unicast conversion function for **DHCP** packets in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize bcmc unicast-send dhcp
```

11.17.13 traffic-optimize bcmc unicast-send mismatch-action drop

Function

The **traffic-optimize bcmc unicast-send mismatch-action drop** command discards broadcast or multicast packets that fail to be converted into unicast packets on air interfaces.

The **undo traffic-optimize bcmc unicast-send mismatch-action drop** command restores the default action, that is, send broadcast or multicast packets that fail to be converted into unicast packets on air interfaces to all users in unicast mode.

By default, if broadcast or multicast packets fail to be converted into unicast packets on air interfaces, the packets are discarded.

Format

traffic-optimize bcmc unicast-send mismatch-action drop

undo traffic-optimize bcmc unicast-send mismatch-action drop

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if broadcast or multicast packets fail to be converted into unicast packets on air interfaces, the packets are discarded. To enable the system to send these packets to all users, run the **undo traffic-optimize bcmc unicast-send mismatch-action drop** command.

Prerequisites

- The **traffic-optimize bcmc unicast-send** command has been executed to configure the function of converting broadcast or multicast packets to unicast packets on an air interface.
- The **undo learn-client-address { ipv4 | ipv6 } disable** command has been executed to enable STA address learning.

Example

Configure the system to send the broadcast or multicast packets that fail to be converted into unicast packets on air interfaces to all users.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] undo traffic-optimize bcmc unicast-send mismatch-action drop
```

11.17.14 traffic-optimize broadcast-suppression

Function

The **traffic-optimize broadcast-suppression** command sets the maximum traffic volume of broadcast packets that can pass through a traffic profile.

The **undo traffic-optimize broadcast-suppression** command cancels the limit on the maximum traffic volume of broadcast packets that can pass through a traffic profile.

By default, broadcast packets are not suppressed in a traffic profile.

Format

traffic-optimize broadcast-suppression packets *packets-rate*

undo traffic-optimize broadcast-suppression

Parameters

Parameter	Description	Value
packets *packets-rate*	Specifies the number of packets transmitted per second.	The value is an integer that ranges from 0 to 14881000, in pps.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of broadcast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected.

To prevent broadcast storms, you can run the **traffic-optimize broadcast-suppression** command to configure the maximum traffic volume of broadcast packets that can pass through a traffic profile. When the traffic volume of broadcast packets reaches the maximum in a traffic profile, the system discards excess broadcast packets to control the traffic volume in a proper range.

Precautions

Traffic suppression on the wireless side takes effect only for incoming traffic on the AP's air interface.

Example

Set the maximum traffic volume of broadcast packets that can pass through to 21600 pps in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize broadcast-suppression packets 21600
```

11.17.15 traffic-optimize multicast-suppression

Function

The **traffic-optimize multicast-suppression** command sets the maximum traffic volume of multicast packets in a traffic profile.

The **undo traffic-optimize multicast-suppression** command cancels the limit on the maximum traffic volume of multicast packets in a traffic profile.

By default, multicast packets are not suppressed in a traffic profile.

Format

traffic-optimize multicast-suppression packets *packets-rate*

undo traffic-optimize multicast-suppression

Parameters

Parameter	Description	Value
packets *packets-rate*	Specifies the number of packets transmitted per second.	The value ranges from 0 to 14881000, in pps.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of multicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected.

To ensure normal service transmission on a network, you can run the **traffic-optimize multicast-suppression** command to configure the maximum multicast traffic volume in a traffic profile. When the traffic volume of multicast packets

reaches the maximum, the system discards excess multicast packets to control the traffic volume in a proper range.

Precautions

Traffic suppression on the wireless side takes effect only for incoming traffic on the AP's air interface.

Example

Set the maximum traffic volume of multicast packets to 21600 pps in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize multicast-suppression packets 21600
```

11.17.16 traffic-optimize multicast-unicast enable

Function

The **traffic-optimize multicast-unicast enable** command enables the multicast-to-unicast conversion function in a traffic profile.

The **undo traffic-optimize multicast-unicast enable** command disables the multicast-to-unicast conversion function in a traffic profile.

By default, the multicast-to-unicast conversion function is disabled in a traffic profile.

NOTE

Multicast-to-unicast conversion of data packets on the air interface is not supported by the following model:

- AirEngine 8771-X1T

Format

traffic-optimize multicast-unicast enable

undo traffic-optimize multicast-unicast enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable the multicast-to-unicast conversion function in scenarios that have high requirements on multicast stream transmission, such as high-definition (HD) video on demand (VOD) scenarios.

After this function is enabled, an AP listens on Report and Leave packets to maintain multicast-to-unicast entries. When sending multicast packets to STAs, the AP converts the multicast packets into unicast packets based on the multicast-to-unicast entries to improve multicast stream transmission efficiency.

Example

Enable the multicast-to-unicast conversion function in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize multicast-unicast enable
```

11.17.17 traffic-optimize multicast-unicast dynamic-adaptive disable

Function

The **traffic-optimize multicast-unicast dynamic-adaptive disable** command disables adaptive multicast-to-unicast conversion in a traffic profile.

The **undo traffic-optimize multicast-unicast dynamic-adaptive disable** command enables adaptive multicast-to-unicast conversion in a traffic profile.

By default, adaptive multicast-to-unicast conversion is enabled in a traffic profile.

NOTE

Multicast-to-unicast conversion of data packets on the air interface is not supported by the following model:

- AirEngine 8771-X1T

Format

traffic-optimize multicast-unicast dynamic-adaptive disable

undo traffic-optimize multicast-unicast dynamic-adaptive disable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After adaptive multicast-to-unicast conversion is enabled, when the air interface performance becomes a bottleneck during multicast-to-unicast conversion, an AP automatically switches the multicast group containing the minimum number of STAs to the multicast mode. After the air interface performance is improved and keeps being improved for a period of time, the AP automatically switches the multicast group containing the maximum number of STAs to the unicast mode. In this way, the air interface performance is automatically adjusted without manual intervention, improving wireless user experience.

Pre-configuration Tasks

The multicast-to-unicast conversion function has been enabled in the traffic profile using the **traffic-optimize multicast-unicast enable** command.

Example

Disable adaptive multicast-to-unicast conversion in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize multicast-unicast enable
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize multicast-unicast dynamic-adaptive disable
```

11.17.18 traffic-optimize nd-proxy enable

Function

The **traffic-optimize nd-proxy enable** command enables ND proxy on the device.

The **undo traffic-optimize nd-proxy enable** command disables ND proxy on the device.

By default, ND proxy is disabled.

Format

traffic-optimize nd-proxy enable

undo traffic-optimize nd-proxy enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an ND Request packet is sent from a user or the network to another user, the AC or AP enabled with ND proxy can reply to this packet. Compared with the function of converting ND multicast packets to unicast packets, ND proxy can reduce the number of times a sleeping terminal is awakened to save power.

Precautions

The ND proxy function is not available for roaming users.

Example

Enable ND proxy on the device in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize nd-proxy enable
```

11.17.19 traffic-optimize sta-bridge-forward disable

Function

The **traffic-optimize sta-bridge-forward disable** command configures the function of denying packets destined for bridge STAs on the air interface.

The **undo traffic-optimize sta-bridge-forward disable** command cancels the function of denying packets destined for bridge STAs on the air interface.

By default, the air interface does not deny packets destined for bridge STAs.

Format

traffic-optimize sta-bridge-forward disable

undo traffic-optimize sta-bridge-forward disable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Some terminals on the wireless network can provide bridging functions. The terminals associate with APs with their MAC addresses and connect to multiple Layer 3 wired devices in the downlink direction. The connected Layer 3 wired devices can also obtain IP addresses and forward traffic through the APs. The APs consider that the associated terminals have multiple IP addresses. You can run the command to configure the function of denying packets destined for bridge STAs on the air interface. This can reduce the number of packets transmitted on the air interfaces and improve the air interface performance.

Example

Configure the function of denying packets destined for bridge STAs on the air interface in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize sta-bridge-forward disable
```

11.17.20 traffic-optimize tcp adjust-mss

Function

The **traffic-optimize tcp adjust-mss** command sets the maximum segment size (MSS) of TCP packets in a traffic profile.

The **undo traffic-optimize tcp adjust-mss** command deletes the configured MSS of TCP packets in a traffic profile.

By default, the MSS of TCP packets in a traffic profile is not configured.

Format

traffic-optimize tcp adjust-mss *value*

undo traffic-optimize tcp adjust-mss

Parameters

Parameter	Description	Value
value	Specifies the MSS of TCP packets in a traffic profile.	The value is an integer that ranges from 128 to 2048, in bytes.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MSS is an option defined in the TCP protocol and refers to the maximum length of TCP packets that can be received by a device. When setting up a TCP connection, the local and peer devices negotiate an MSS value to determine the maximum data length of TCP packets. If the length of TCP packets sent from the peer device exceeds the MSS value, the packets are fragmented.

Precautions

- To prevent TCP packets from being fragmented, you must configure a proper MSS based on the maximum transmission unit (MTU). The MTU is the option to determine whether IP packets will be fragmented. If the size of an IP packet exceeds the MTU, the IP packet will be fragmented. To ensure that a complete packet is transmitted properly, the MSS value plus all the header lengths (TCP header and IP header) cannot exceed the MTU. For example, a CAPWAP-encapsulated TCP packet consists of an outer IP header (20 bytes), a UDP header (8 bytes), a CAPWAP header (8 bytes), an ETH header (18 bytes), an inner IP header (20 bytes), a TCP header (20 bytes), and TCP data. If the default MTU is 1500 on the device, the MSS value can be set to a maximum of 1406 bytes so that the CAPWAP-encapsulated TCP packet is not fragmented by the device. In case that the CAPWAP header or TCP header carries option fields, it is recommended that you set the MSS to 1380 bytes.
- The MSS configured by the **traffic-optimize tcp adjust-mss** command takes effect on the AP as a TCP client or server. Additionally, if packets of other devices as clients pass through the AP, the negotiation result is modified based on the MSS configured using this command only when the MSS received by the AP is larger than that configured using this command.
- If you run the **traffic-optimize tcp adjust-mss** command in the same interface view multiple times, only the latest configuration takes effect.

Example

Set the MSS of TCP packets to 1200 bytes in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize tcp adjust-mss 1200
```

11.17.21 traffic-optimize unicast-suppression

Function

The **traffic-optimize unicast-suppression** command sets the maximum traffic volume of unknown unicast packets in a traffic profile.

The **undo traffic-optimize unicast-suppression** command cancels the limit on the maximum traffic volume of unknown unicast packets in a traffic profile.

By default, unknown unicast packets are not suppressed in a traffic profile.

Format

traffic-optimize unicast-suppression packets *packets-rate*

undo traffic-optimize unicast-suppression

Parameters

Parameter	Description	Value
packets *packets-rate*	Specifies the number of packets transmitted per second.	The value ranges from 0 to 14881000, in pps.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of unknown unicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected.

To prevent broadcast storms, you can run the **traffic-optimize unicast-suppression** command to configure the maximum traffic volume of unknown unicast packets that can pass through an interface. When the traffic volume of unknown unicast packets reaches the maximum on an interface, the system discards excess unknown unicast packets to control the traffic volume in a proper range.

Precautions

Traffic suppression on the wireless side takes effect only for incoming traffic on the AP's air interface.

Example

Set the maximum traffic volume of unknown unicast packets to 21600 pps in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize unicast-suppression packets 21600
```

11.18 Centralized License Control Commands

11.18.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.18.2 license centralized enable

Function

The **license centralized enable** command enables centralized license control.

The **undo license centralized enable** command disables centralized license control.

By default, centralized license control is disabled.

Format

license centralized enable

undo license centralized enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When centralized license control is enabled on both the license server and license clients, licenses in the license resource pool can be centrally controlled on the license server and shared by both the license server and license clients.

Example

Enable centralized license control.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] license centralized enable
```

11.18.3 license server

Function

The **license server** command specifies the IP address of the license server on a license client. This IP address must be the same as the CAPWAP source address configured on the license server.

The **undo license server** command deletes the local IP address of the license server on a license client.

By default, no IP address is set for the license server.

Format

license server ip-address *ip-address*

undo license server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IPv4 address of the license server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After centralized license control is enabled, you can run the **license server** command on a license client to set an IP address for the license server, so that the license client can set up a link with the license server and be managed by the license server.

Prerequisites

The local IP address of the license client has been configured. Run the **license client source ip-address** *ip-address* command to configure the local IP address of the license client.

- When multiple CAPWAP source addresses exist, use this configuration to specify one CAPWAP source address as the local address.
- If the license client is a single device, the source address configuration is not required. Instead, the CAPWAP source address is used as the local address of the license client by default.

Example

Set the IP address for the license server to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] license server ip-address 10.1.1.1
```

11.18.4 license client source

Function

The **license client source** command configures a local IP address for a license client.

The **undo license client source** command deletes the local IP address of a license client.

By default, the first CAPWAP source IP address is used as the local IP address of a license client.

Format

license client source ip-address *ip-address*

undo license client source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the local IPv4 address of the license client.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When multiple CAPWAP source addresses exist, use this configuration to specify one CAPWAP source address as the local address.
- If the license client is a single device, the source address configuration is not required. Instead, the CAPWAP source address is used as the local address of the license client by default.

Example

Set the local IP address of a license client to 10.1.2.1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] license client source ip-address 10.1.2.1
```

11.18.5 display license centralized configuration

Function

The **display license centralized configuration** command displays the configuration of centralized license control.

Format

display license centralized configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check whether centralized license control is enabled and the IP address of the license server.

Example

Display the configuration of centralized license control on the license server.

```
<HUAWEI> display license centralized configuration
-------------------------------------------------
License centralized server enable :    enable
License server IP                 :    -
-------------------------------------------------
```

Display the configuration of centralized license control on a license client.

```
<HUAWEI> display license centralized configuration
-------------------------------------------------
License centralized server enable :    enable
License server IP                 :    10.1.1.1
License local IP                  :    10.1.1.2
-------------------------------------------------
```


Table 11-311 Description of the **display license centralized configuration** command output

Item	Description
License centralized server enable	Whether centralized license control is enabled. • enable: Centralized license control is enabled. • disable: Centralized license control is disabled. To configure this parameter, run the **license centralized enable** command.
License server IP	IP address of the license server. To configure this parameter on a license client, run the **license server** command.
License local IP	Local IP address of the license client. To configure this parameter on a license client, run the **license client source** command. If this parameter is not configured, **-** is displayed.

11.18.6 display license resource usage detail

Function

The **display license resource usage detail** command displays the license resource usage in the license resource pool or on a single AC.

Format

display license resource usage detail

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

- If centralized license control is enabled, you can run this command on the license server to check the license resource usage in the license resource pool, on all license servers, and on all license clients. On a license client, you can run this command to check the license resource usage in the license resource pool and on the local AC.
- When centralized license control is disabled, you can run this command to check the license resource usage on the local AC and backup AC.

Example

Display the license resource usage on a license server.

```
<HUAWEI> display license resource usage detail
Remain(days): Remaining days of the license resource pool after the client goes offline
Current role       : server
Used/Total resource:  300/1100
--------------------------------------------------------------------------------------------------
MAC               Role          State    Local License  Used     Remain(days)    IP
--------------------------------------------------------------------------------------------------
0000-0000-0015    server         normal   100            200      -               -
0000-0000-0017    client         normal   600            100      -               1.1.1.3
0000-0000-0018    client         fault    100            -        20              1.1.1.5
--------------------------------------------------------------------------------------------------
Total records: 4
```

Display the license resource usage on a license client.

```
<HUAWEI> display license resource usage detail
Remain(days): Remaining days of the license resource pool after the client goes offline
Current role       : client
Used/Total resource:  300/1100
--------------------------------------------------------------------------------------------------
MAC               Role          State    Local License  Used     Remain(days)    IP
--------------------------------------------------------------------------------------------------
0000-0000-0023    client         normal   600            100      -               1.1.1.3
--------------------------------------------------------------------------------------------------
Total records: 1
```

Display the license resource usage on an AC when centralized license control is not in effect.

```
<HUAWEI> display license resource usage detail
Remaining days: Remaining days of the backup license
Used/Total resource    :    0/4
--------------------------------------------------------------------------------------------------
 AC MAC           License     Backup Time                Remaining Days    Backup Mode
--------------------------------------------------------------------------------------------------
 Local AC         4           -                          -                 -
--------------------------------------------------------------------------------------------------
Total records: 1
```

Table 11-312 Description of the **display license resource usage detail** command output

Item	Description
Current role	Role of the current AC. • server • client

Item	Description
Used/Total resource	License resource usage, that is, ratio of the number of used licenses to the total number of licenses.
MAC	MAC address of an AC.
Role	Role of an AC. • server • client
State	State of the link between a license client and the license server. • normal: The license client is properly connected to the license server. • fault: The license client is disconnected from the license server.
Local License	Number of loaded licenses on an AC.
Used	Number of used licenses on an AC.
Remain(days)	Remaining days of the license resource pool after the license client is disconnected from the license server.
IP	IP address used by a license client to set up a link with the license server.
AC MAC	MAC address of the backup AC. **Local AC** indicates the local AC.
License	Number of loaded licenses on the AC.
Backup Time	Time when licenses are backed up. This field is unavailable currently and is displayed as **-**.
Remaining Days	Remaining days of the backup license. This field is unavailable currently and is displayed as **-**.
Backup Mode	Backup mode. This field is unavailable currently and is displayed as **-**.

11.19 WLAN Reliability Commands

11.19.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.19.2 ac protect alarm-restrain enable

Function

The **ac protect alarm-restrain enable** command enables AP Fault alarm suppression.

The **undo ac protect alarm-restrain enable** command disables AP Fault alarm suppression.

By default, AP Fault alarm suppression is disabled.

Format

ac protect alarm-restrain enable

undo ac protect alarm-restrain enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In dual-link cold backup scenarios, after an AP becomes **Fault** on the active AC, switches to the standby AC, and works properly, the active AC generates an AP Fault alarm. If AP Fault alarms are not needed in this case, you can run this command to enable AP Fault alarm suppression.

After AP Fault alarm suppression is enabled, the active and standby ACs generate AP Fault alarms only when both ACs detect that an AP becomes faulty on them.

Precautions

The active and standby ACs notify each other of the AP status by exchanging packets. If communication between the ACs fails, AP Fault alarm suppression cannot take effect.

AP Fault alarm suppression can only suppress the AP Fault alarms caused by heartbeat timeout. If an AP is deleted or restarted using the **undo ap** or **ap-reset** command, the alarms cannot be suppressed.

Example

Enable AP Fault alarm suppression.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect alarm-restrain enable
```

11.19.3 ac protect cold-backup kickoff-station

Function

The **ac protect cold-backup kickoff-station** command enables the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured.

The **undo ac protect cold-backup kickoff-station** command restores the default setting.

By default, STAs using open system authentication remain connected to APs when an active/standby AC switchover is implemented.

Format

ac protect cold-backup kickoff-station

undo ac protect cold-backup kickoff-station

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

An active/standby switchover between two ACs that have dual-link cold backup configured causes a short service interruption.

- STAs not using open system authentication are disconnected from APs and need to go online again after the active/standby switchover.
- By default, STAs using open system authentication remain connected to APs and do not need to go online again after the active/standby switchover. You can run the **ac protect cold-backup kickoff-station** command to configure the STAs to be disconnected when an active/standby AC switchover is implemented.

Example

Enable the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect cold-backup kickoff-station
```

11.19.4 ac protect link-switch packet-loss echo-probe-time

Function

The **ac protect link-switch packet-loss echo-probe-time** command specifies the number of Echo packets sent within a statistics collection interval.

The **undo ac protect link-switch packet-loss echo-probe-time** command restores the default number of Echo packets sent within a statistics collection interval.

By default, the number of Echo packets sent within a statistics collection interval is 20.

Format

ac protect link-switch packet-loss echo-probe-time *echo-probe-time*

undo ac protect link-switch packet-loss echo-probe-time

Parameters

Parameter	Description	Value
echo-probe-time	Specifies the number of Echo packets.	The value is an integer that ranges from 6 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active/standby link switchover mode is set to the network stabilization mode, ACs periodically check whether the network stabilization of active and standby links meets the condition for triggering an active/standby link switchover

and collect statistics about the specified number of Echo packets at each interval to calculate the network stabilization.

In N+1 backup scenarios, only one of the primary and backup ACs sets up a CAPWAP link with an AP at the same time. The network stabilization of this link can be calculated through Echo packets. The network stabilization of the link between the AP and another AC can be calculated through Primary Discovery packets. Statistics about Primary Discovery packets can also be collected by setting the parameter *echo-probe-time*.

Prerequisites

The active/standby link switchover mode has been set to the network stabilization mode using the **ac protect link-switch mode network-stabilization** command.

Example

Set the number of Echo packets sent within a statistics collection interval to 30.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name abc
[HUAWEI-wlan-ap-system-prof-abc] ac protect link-switch packet-loss echo-probe-time 30
```

11.19.5 ac protect link-switch mode

Function

The **ac protect link-switch mode** command configures the active/standby link switchover mode.

The **undo ac protect link-switch mode** command restores the default active/standby link switchover mode.

By default, the active/standby link switchover mode is the priority mode.

Format

ac protect link-switch mode { **priority** | **network-stabilization** }

undo ac protect link-switch mode

Parameters

Parameter	Description	Value
priority	Sets the active/standby link switchover mode to the priority mode.	-
network-stabilization	Sets the active/standby link switchover mode to the network stabilization mode.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In dual-link cold backup or hot standby scenarios, an AP simultaneously sets up active and standby links with active and standby ACs, respectively. If the active link is faulty, the AP switches service traffic to the standby link and goes online on the standby AC. When the active link recovers, the AP detects that this link has a higher priority than the other one and triggers a revertive switchover. After 20 Echo intervals, the AP switches service traffic back to the active AC.

- To enable an AP to preferentially switch service traffic to the active link, set the active/standby link switchover mode to the priority mode.
- To allow an AP to use a link with high network stabilization, set the active/standby link switchover mode to the network stabilization mode. When the condition for triggering an active/standby link switchover is met, the AP preferentially switches service traffic to the link on a network with higher stabilization. In this case, whether an active/standby link switchover is performed is only related to the network stabilization of links but not related to the active and standby roles of links. You can run the **ac protect link-switch packet-loss** { **gap-threshold** *gap-threshold* | **start-threshold** *start-threshold* } command to configure the condition for triggering an active/standby link switchover.

In N+1 backup scenarios, APs set up links only with the primary ACs. When a link between an AP and a primary AC fails, the AP sets up a link with the backup AC and goes online on the backup AC. When the primary AC is recovered, a revertive switchover is triggered. The AP switches the link back to the primary AC after 20 Echo intervals.

- To enable an AP to preferentially go online on the primary AC, set the active/standby link switchover mode to the priority mode.
- To allow an AP to use a link with high network stabilization, set the active/standby link switchover mode to the network stabilization mode.

Precautions

The active/standby link switchover mode applies to active and standby ACs configured using the **ac protect protect-ac** and **priority** commands, or the **primary-access** and **backup-access** commands.

Example

Set the active/standby link switchover mode to the network stabilization mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name abc
[HUAWEI-wlan-ap-system-prof-abc] ac protect link-switch mode network-stabilization
```


11.19.6 ac protect link-switch packet-loss

Function

The **ac protect link-switch packet-loss** command configures the packet loss rate start and difference thresholds for an active/standby link switchover.

The **undo ac protect link-switch packet-loss** command restores the default packet loss rate start and difference thresholds for an active/standby link switchover.

By default, the packet loss rate start and difference thresholds for an active/standby link switchover are 20% and 15%, respectively.

Format

ac protect link-switch packet-loss { **gap-threshold** *gap-threshold* | **start-threshold** *start-threshold* }

undo ac protect link-switch packet-loss { **gap-threshold** | **start-threshold** }

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold*	Specifies the packet loss rate difference threshold for an active/standby link switchover.	The value is an integer that ranges from 5 to 60, in percentage.
start-threshold *start-threshold*	Specifies the packet loss rate start threshold for an active/standby link switchover.	The value is an integer that ranges from 5 to 60, in percentage.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active/standby link switchover mode is set to the network stabilization mode, ACs check whether the network stabilization of active and standby links meets the condition for triggering an active/standby link switchover. If so, service traffic is switched to the link with higher network stabilization. If not, the switchover is not performed.

In dual-link cold backup and hot standby scenarios, the network stabilization of active and standby links is determined based on the Echo packet loss rate. The active/standby link switchover is performed when the following conditions are met:

1. APs collect statistics about the specified number of Echo packets forwarded through the link in use at each interval and find that the calculated packet loss rate is higher than the packet loss rate start threshold.
2. The packet loss rate of the link in use is higher than that of the other link, and the difference between the two links' packet loss rates is higher than the packet loss rate difference threshold.

In N+1 backup scenarios, the network stabilization of the link between an AP and the current AC is determined by the Echo packet loss rate, and that of the link between the AP and another AC is determined by the Primary Discovery packet loss rate. The conditions for triggering an active/standby switchover are the same as those for dual-link cold backup and hot standby scenarios.

Prerequisites

The active/standby link switchover mode has been set to the network stabilization mode using the **ac protect link-switch mode network-stabilization** command.

Example

Set the packet loss rate start threshold for an active/standby link switchover to 30%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name abc
[HUAWEI-wlan-ap-system-prof-abc] ac protect link-switch packet-loss start-threshold 30
```

11.19.7 ac protect enable

Function

The **ac protect enable** command enables dual-link backup globally and disables N+1 backup.

The **undo ac protect enable** command disables dual-link backup globally and enables N+1 backup.

By default, dual-link backup is disabled globally, and N+1 backup is enabled.

Format

ac protect enable

undo ac protect enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure service stability, an AP needs to establish connections with two ACs. The two ACs work in active/standby mode. The active AC provides services for APs, whereas the standby AC is a backup to the active AC.

Follow-up Procedure

After dual-link backup or N+1 backup is enabled globally, configure the AC priority and standby AC IP address to implement dual-link backup or N+1 backup.

Precautions

Ensure that active and standby ACs deliver the same WLAN service configuration to an AP that connects to the two ACs.

Example

Enable dual-link backup globally and disable N+1 backup.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect enable
Warning: This operation maybe cause AP reset, continue?[Y/N]:y
```

11.19.8 ac protect priority

Function

The **ac protect priority** command configures the AC priority in the WLAN view.

The **undo ac protect priority** command restores the default AC priority in the WLAN view.

By default, the AC priority in the WLAN view is 0.

Format

ac protect priority *priority*

undo ac protect priority

Parameters

Parameter	Description	Value
priority	Specifies the AC priority.	The value is an integer that ranges from 0 to 7. A smaller value indicates a higher priority.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP goes online, ACs deliver their priorities to the AP. The AP selects the AC with a higher priority as the active AC and establishes a CAPWAP tunnel with the active AC.

To implement dual-link backup on all the APs connected to an AC, configure the AC priority and standby AC IP address in the WLAN view to reduce the configuration workload.

Precautions

If the AC priority is configured in the WLAN view and AP system profile view before an AP goes online, the AC priority configured in the AP system profile view is delivered to the AP. If no AC priority is configured in the AP system profile view, the AC priority configured in the WLAN view is delivered to the AP.

Example

Set the AC priority to 3 in the WLAN view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect priority 3
```

11.19.9 ac protect protect-ac

Function

The **ac protect protect-ac** command configures the standby AC IP address in the WLAN view.

The **undo ac protect protect-ac** command restores the default standby AC IP address in the WLAN view.

By default, no standby AC IP address is configured in the WLAN view.

Format

ac protect protect-ac *ip-address*

undo ac protect protect-ac

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address for the standby AC.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement dual-link backup on all the APs connected to an AC, configure the AC priority and standby AC IP address in the WLAN view to reduce the configuration workload.

Precautions

If standby AC IP addresses are configured in both the WLAN view and AP system profile view before an AP goes online, the standby AC IP address configured in the AP system profile view is delivered to an AP. If no standby AC IP address is configured in the AP system profile view, the standby AC IP address configured in the WLAN view is delivered to an AP. If no standby AC IP address is configured in the WLAN view, dual-link backup is disabled.

The standby AC's IP address must be set to the same as the CAPWAP source address of the standby AC.

Example

Set the standby AC IP address to 10.33.12.56 in the WLAN view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect protect-ac 10.33.12.56
```

11.19.10 ac protect restore disable

Function

The **ac protect restore disable** command disables global revertive switching.

The **undo ac protect restore disable** command enables global revertive switching.

By default, global revertive switching is enabled.

Format

ac protect restore disable

undo ac protect restore disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AC1 is the active AC and AC2 is the standby AC. When the link between AC1 and an AP fails, AC2 takes the active role.

When the link between AC1 and the AP recovers, the AP detects that AC1 priority is higher than AC2 and instructs AC1 and AC2 to perform revertive switching. AC1 then becomes the active AC again.

Precautions

- The **undo wlan ac protect restore disable** command must be used before an AP goes online and dual-link backup is implemented. In this way, the AC delivers the revertive switching configuration to the AP when the AP goes online.
- If global revertive switching is disabled, traffic of an AP cannot be switched back to AC1 when the link between AC1 and the AP restores.
- The command takes effect after an AP restart.

Example

Disable global revertive switching.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect restore disable
```

11.19.11 backup-access

Function

The **backup-access** command configures a backup AC IP address.

The **undo backup-access** command restores the default backup AC IP address.

By default, no backup AC IP address is configured.

Format

backup-access ip-address *ip-address*

undo backup-access

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address of the backup AC.	The value is in dotted decimal notation.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In AC backup scenarios, a backup AC IP address is configured so that APs can establish CAPWAP tunnels to the backup AC if they fail to establish CAPWAP tunnels to the primary AC.

Precautions

- The configurations of **primary-access** and **backup-access** take effect only if both the commands are run to configure different IP addresses.
- **primary-access** and **backup-access** cannot be configured with **priority** or **protect-ac**.
- It is not recommended that **primary-access** and **backup-access** be configured with **ac protect protect-ac** or **ac protect priority**.
- The configuration takes effect only after the AP is restarted.
- The IP addresses specified by **primary-access** and **backup-access** must be configured the same as CAPWAP source IP addresses. If the CAPWAP source addresses have been translated using NAT, set the **primary-access** and **backup-access** IP addresses to the translated addresses.

Example

Set the backup AC IP address to 10.33.12.78.

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



```
[HUAWEI-wlan-view] ap-system-profile name sys1
[HUAWEI-wlan-ap-system-prof-sys1] backup-access ip-address 10.33.12.78
```

11.19.12 display ac protect

Function

The **display ac protect** command displays AC dual-link backup configuration.

Format

display ac protect

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view AC dual-link backup configuration.

Example

Display AC dual-link backup configuration.

```
<HUAWEI> display ac protect
------------------------------------------------------------
Protect state             : disable
Protect AC                : -
Priority                  : 0
Protect restore           : enable
Coldbackup kickoff station: disable
Alarm restrain            : disable
------------------------------------------------------------
```


Table 11-313 Description of the **display ac protect** command output

Item	Description
Protect state	Whether global dual-link backup and N+1 backup are enabled. • disable: Global dual-link backup is disabled, and N+1 backup is enabled. • enable: Global dual-link backup is enabled, and N+1 backup is disabled. To configure the parameter, run the **ac protect enable** command.
Protect AC	Standby AC IP address. To configure the parameter, run the **ac protect protect-ac** command.
Priority	Priority of the local AC. To configure the parameter, run the **ac protect priority** command.
Protect restore	Whether global revertive switching is enabled on the AC. To configure the parameter, run the **ac protect restore disable** command.
Coldbackup kickoff station	Whether to enable the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured. To configure the parameter, run the **ac protect cold-backup kickoff-station** command.
Alarm restrain	Whether to enable AP fault alarm suppression. To configure the parameter, run the **ac protect alarm-restrain enable** command.

11.19.13 primary-access

Function

The **primary-access** command configures a primary AC IP address.

The **undo primary-access** command restores the default primary AC IP address.

By default, no primary AC IP address is configured.

Format

primary-access ip-address *ip-address*

undo primary-access

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address of the primary AC.	The value is in dotted decimal notation.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In AC backup scenarios, a primary AC IP address is configured. When APs attempt to go online, they preferentially associate with the primary AC and establish CAPWAP tunnels.

Precautions

- The configurations of **primary-access** and **backup-access** take effect only if both the commands are run to configure different IP addresses.
- **primary-access** and **backup-access** cannot be configured with **priority** or **protect-ac**.
- It is not recommended that **primary-access** and **backup-access** be configured with **ac protect protect-ac** or **ac protect priority**.
- The configuration takes effect only after the AP is restarted.
- The IP addresses specified by **primary-access** and **backup-access** must be configured the same as CAPWAP source IP addresses. If the CAPWAP source addresses have been translated using NAT, set the **primary-access** and **backup-access** IP addresses to the translated addresses.

Example

Set the primary AC IP address to 10.33.12.56.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name sys1
[HUAWEI-wlan-ap-system-prof-sys1] primary-access ip-address 10.33.12.56
```


11.19.14 priority

Function

The **priority** command sets the AC priority in the AP system profile view.

The **undo priority** command restores the AC priority to the default setting in the AP system profile view.

By default, no AC priority is configured in the AP system profile view.

Format

priority *priority-level*

undo priority

Parameters

Parameter	Description	Value
priority-level	Specifies the AC priority.	The value is an integer that ranges from 0 to 7. A smaller value indicates a higher priority.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP goes online, ACs deliver their priorities to the AP. The AP selects the AC with the highest priority as the active AC and establishes a CAPWAP tunnel with the active AC.

Precautions

If the AC priority is configured in the WLAN view and AP system profile view before an AP goes online, the AC priority configured in the AP system profile view is delivered to the AP. If no AC priority is configured in the AP system profile view, the AC priority configured in the WLAN view is delivered to the AP.

If ACs deliver the same priorities to the AP, the AP selects the AC with the lowest AP load as the active AC. If both AC priorities and AP load are the same, the AP selects the AC with the lowest STA load as the active AC. If AC priorities, AP load, and STA load are the same, the AP selects the AC with the smallest IP address as

the active AC to establish a CAPWAP tunnel. The AP or STA load equals the number of allowed APs or STAs minus the number of existing APs or STAs.

Example

Set the AC priority to 3 in the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] priority 3
```

11.19.15 protect-ac

Function

The **protect-ac** command configures the standby AC's IP address in the AP system profile view.

The **undo protect-ac** command restores the standby AC's IP address to the default setting in the AP system profile view.

By default, no standby AC's IP address is configured in the AP system profile view.

Format

protect-ac ip-address *ip-address*

undo protect-ac

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address for the standby AC.	The value is in dotted decimal notation.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable an AP to establish connections with two ACs (active and standby ACs) to implement dual-link backup, you can run this command to configure the standby AC IP address in the AP system profile view.

Precautions

If standby AC's IP addresses are configured in both the WLAN view and AP system profile view, the standby AC's IP address configured in the AP system profile view is delivered to an AP. If no standby AC's IP address is configured in the AP system profile view, the standby AC's IP address configured in the WLAN view is delivered to an AP.

The IP address of the standby AC cannot be specified as the IP address of the local device. Otherwise, the backup function does not take effect.

The standby AC's IP address must be set to the same as the CAPWAP source address of the standby AC.

Example

Set the standby AC's IP address to 10.3.3.3 in the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] protect-ac ip-address 10.3.3.3
```

11.20 WMI Commands

11.20.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.20.2 ap log module

Function

The **ap log module** command enables APs to report logs of the module with a specified ID to a WMI server.

The **undo ap log module mid** *mid* command disables APs from reporting logs of the module with a specified ID to a WMI server.

The **undo ap log module all** command disables APs from reporting logs of all modules to a WMI server.

By default, APs do not report logs of any module to a WMI server.

Format

ap log module mid *mid* [**name** *name*]

undo ap log module { **mid** *mid* | **all** }

Parameters

Parameter	Description	Value
mid *mid*	Specifies a module ID.	The value is in hexadecimal notation. Set the value to the ID of a module registered with the information center. **NOTE** You can enter **mid ?** to obtain the predefined ID of a module and the module name. You can run the **display info-center statistics** command on an AP to query more module IDs.
name *name*	Specifies a module name. The value must correspond to the value of **mid**.	The value is a string of 1 to 24 characters.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

If APs need to report logs to a WMI server, specify the ID of a module whose logs are to be reported and enable the log report function. Otherwise, the APs do not report logs of this module.

To enable APs to report logs of multiple modules, run this command repeatedly to specify multiple module IDs.

Example

Enable APs to report logs of the module **C1480000** to a WMI server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] ap log module mid c1480000
```

11.20.3 collect-item (WMI profile view)

Function

The **collect-item** command configures whether APs report collected data to a WMI server and specifies the data collection interval.

The **undo collect-item** command restores the default configuration for APs to report collected data to a WMI server and restores the default data collection interval.

Table 11-314 lists the default state of whether APs report data to the WMI server and the default data collection intervals. (The default values are recommended.)

Table 11-314 Default settings of the data reporting function and data collection interval

Data Type	Default State	Default Data Collection Interval (Unit: Second)
Site guest data	Enabled	300
CPCAR data	Enabled	300
Device monitoring data	Enabled	10
Enhanced Media Delivery Index (eMDI) data	Enabled	10
Interface monitoring data	Enabled	60
Wireless device location data	Disabled	60
Log data	Enabled	300
Radio data of neighboring wireless devices	Enabled	60
Radio monitoring data	Enabled	10
SSID monitoring data	Enabled	60
STA data	Enabled	10
AI roaming data	Enabled	300
DHCP option information about STAs	Disabled	300
User agent (UA) information in the HTTP packets sent by STAs.	Disabled	300
Service information in the mDNS packets sent by STAs	Disabled	300
DNS data	Disabled	60
Non-Wi-Fi device information	Disabled	60

Data Type	Default State	Default Data Collection Interval (Unit: Second)
iPCA 2.0 measurement information	Enabled	Real-time
LLDP neighbor data	Enabled	Real-time
Spectrum analysis data	Disabled	Real-time

Format

collect-item { **application-statistics-data** | **cpcar-data** | **device-data** | **emdi-data** | **interface-data** | **log-data** | **neighbor-device-data** | **radio-data** | **ssid-data** | **terminal-data** | **ai-roam-data** } { **interval** *interval* | **disable** }

undo collect-item { **application-statistics-data** | **cpcar-data** | **device-data** | **emdi-data** | **interface-data** | **log-data** | **neighbor-device-data** | **radio-data** | **ssid-data** | **terminal-data** | **ai-roam-data** }

collect-item { **location-data** | **terminal-dhcp-option-data** | **terminal-http-ua-data** | **terminal-mdns-data** | **dns-data** | **non-wifi-data** } { **interval** *interval* | **enable** }

undo collect-item { **location-data** | **terminal-dhcp-option-data** | **terminal-http-ua-data** | **terminal-mdns-data** | **dns-data** | **non-wifi-data** }

collect-item { **s-ipfpm-data** | **lldp-data** } **disable**

undo collect-item { **s-ipfpm-data** | **lldp-data** } **disable**

collect-item spectrum-data enable

undo collect-item spectrum-data enable

Parameters

Parameter	Description	Value
application-statistics-data	Indicates site guest data. This parameter is not supported by RUs.	-
cpcar-data	Indicates CPCAR data.	-
device-data	Indicates device monitoring data.	-
emdi-data	Indicates eMDI data. This parameter is not supported by Fit central APs or RUs.	-

Parameter	Description	Value
interface-data	Indicates interface monitoring data.	-
location-data	Indicates wireless device location data. This parameter is not supported by Fit central APs.	-
log-data	Indicates log data.	-
neighbor-device-data	Indicates radio data of neighboring wireless devices. This parameter is not supported by Fit central APs.	-
radio-data	Indicates radio monitoring data. This parameter is not supported by Fit central APs.	-
ssid-data	Indicates SSID monitoring data. This parameter is not supported by Fit central APs.	-
terminal-data	Indicates STA data. This parameter is not supported by Fit central APs.	-
ai-roam-data	Indicates AI roaming data.	-
terminal-dhcp-option-data	Indicates DHCP Option information (Options 12, 55, and 60) in the DHCP packets sent by STAs.	-
terminal-http-ua-data	Indicates UA information in the HTTP packets sent by STAs.	-
terminal-mdns-data	Indicates service information in the mDNS packets sent by STAs.	-
dns-data	Indicates DNS information. **NOTE** DNS information can be reported from APs only to iMaster NCE-CampusInsight.	-

Parameter	Description	Value
non-wifi-data	Indicates non-Wi-Fi device information.	-
s-ipfpm-data	Indicates iPCA 2.0 measurement information.	-
lldp-data	Indicates LLDP neighbor data. **NOTE** LLDP neighbor data of APs can be reported only to iMaster NCE-Campus.	-
spectrum-data	Indicates spectrum analysis data.	-
interval *interval*	Specifies the data collection interval.	The value is an integer, in seconds. The value range is as follows: • **location-data**: 1 to 1800 • Other data: 5 to 1800
disable	Disables APs from reporting collected data to the WMI server.	-
enable	Enables APs to report collected data to the WMI server.	-

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure APs to report collected data to the WMI server and set the data collection interval as required. You can run this command multiple times to configure APs to report different types of data to the WMI server.

Precautions

For APs that can only transparently report collected information, the collection interval is fixed at 5 minutes, and is unconfigurable.

Example

Set the interval for collecting device monitoring data to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] collect-item device-data interval 500
```

11.20.4 collect-location-data enable

Function

The **collect-location-data enable** command enables the device to collect wireless device location data.

The **undo collect-location-data enable** command disables the device from collecting wireless device location data.

By default, the device does not collect wireless device location data.

Format

collect-location-data enable

undo collect-location-data enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to enable the device to collect and report wireless device location data to a WMI server for customer flow analysis.

Example

Enable the device to collect wireless device location data.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name default
[HUAWEI-wlan-location-prof-default] collect-location-data enable
```

11.20.5 collect-location-data rssi-threshold

Function

The **collect-location-data rssi-threshold** command configures the RSSI threshold for wireless device location data.

The default RSSI threshold for wireless device location data is -75 dBm.

Format

collect-location-data rssi-threshold *rssi-threshold*

Parameters

Parameter	Description	Value
rssi-threshold	Specifies an RSSI threshold.	The value is an integer that ranges from -95 to 0, in dBm.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

After the device is enabled to collect wireless device location data, only data with the RSSI of higher than the threshold is collected.

Example

Set the RSSI threshold for wireless device location data to -72 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name default
[HUAWEI-wlan-location-prof-default] collect-location-data rssi-threshold -72
```

11.20.6 display references wmi-server

Function

The **display references wmi-server** command displays reference information about a WMI profile.

Format

display references wmi-server name *wmi-server-name*

Parameters

Parameter	Description	Value
name *wmi-server-name*	Displays reference information about a specified WMI profile.	The WMI profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wmi-server** command to view reference information about a WMI profile.

Example

Display reference information about the WMI profile **abc**.

```
<HUAWEI> display references wmi-server name abc
------------------------------------------------------------------------------
Reference type              Reference name              Reference Index
------------------------------------------------------------------------------
AP system profile           a                           1
------------------------------------------------------------------------------
Total: 1
```

Table 11-315 Description of the **display references wmi-server name** *wmi-server-name* command output

Item	Description
Reference type	Type of the profile by which a WMI profile is referenced.
Reference name	Name of the profile by which a WMI profile is referenced.
Reference Index	Index for referencing a WMI profile to the AP system profile.

11.20.7 display wmi-server

Function

The **display wmi-server** command displays configuration and reference information about a WMI profile.

Format

display wmi-server { **all** | **name** *wmi-server-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WMI profiles.	-
name *wmi-server-name*	Displays information about a specified WMI profile.	The WMI profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about a WMI profile.

Example

Display information about all WMI profiles.

```
<HUAWEI> display wmi-server all
-------------------------------------------------------
Profile name                    Reference
-------------------------------------------------------
abc                          0
-------------------------------------------------------
Total: 1
```

Table 11-316 Description of the **display wmi-server all** command output

Item	Description
Profile name	Name of a WMI profile.
Reference	Number of times a WMI profile is referenced.

Display information about the WMI profile **abc**.

```
<HUAWEI> display wmi-server name abc
-------------------------------------------------------------------------------
Server ip                       : 10.10.10.10
Server port                      : 10032
```



```
Server backup ip                    : 10.10.10.11
Server backup port                   : 10032
Report interval(s)                  : 60
Max packet-size(Kbyte)                : 5
Alive interval(min)                 : 3
Retry interval(min)                  : 5
Retry number                        : 0
Device enable                       : enable
Device data interval(s)               : 10
Ssid enable                         : enable
Ssid data interval(s)                : 60
Radio enable                        : enable
Radio data interval(s)               : 10
Interface enable                    : enable
Interface data interval(s)           : 60
Terminal enable                     : enable
Terminal data interval(s)             : 10
Log enable                          : enable
Log data interval(s)                 : 300
Location enable                     : disable
Neighbor device enable                : enable
Neighbor device data interval(s)       : 60
CP-CAR enable                       : enable
CP-CAR data interval(s)               : 300
EMDI enable                         : enable
EMDI data interval(s)                : 10
Application statistics enable         : enable
Application statistics data interval(s): 300
Terminal DHCP option enable           : enable
Terminal DHCP option data interval(s)  : 300
Terminal HTTP UA enable               : enable
Terminal HTTP UA data interval(s)      : 300
Terminal mDNS enable                  : enable
Terminal mDNS data interval(s)         : 300
DNS enable                          : enable
DNS data interval(s)                  : 50
Non WiFi data enable                   : enable
Non WiFi data interval(s)              : 60
Log module ID                       : C1480000
S-ipfpm enable                      : enable
AI roam data enable                    : enable
AI roam data interval(s)               : 300
Lldp enable                         : enable
PKI realm                           : default
Spectrum data enable                   : disable
------------------------------------------------------------------------------
```

Table 11-317 Description of the **display wmi-server name** command output

Item	Description
Server ip	IP address of the primary WMI server. To configure this parameter, run the **server ip-address** *ip-address* **port** *port* (WMI profile view) command.
Server port	Port number of the primary WMI server. To configure this parameter, run the **server ip-address** *ip-address* **port** *port* (WMI profile view) command.
Server backup ip	IP address of the backup WMI server. To configure this parameter, run the **server backup ip-address** *ip-address* **port** *port* (WMI profile view) command.

Item	Description
Server backup port	Port number of the backup WMI server. To configure this parameter, run the **server backup ip-address** *ip-address* **port** *port* (WMI profile view) command.
Report interval(s)	Data report interval. To configure this parameter, run the **report-interval** *interval* (WMI profile view) command.
Max packet-size(Kbyte)	Maximum size of reported data. To configure this parameter, run the **max-packet-size** *size* (WMI profile view) command.
Alive interval(min)	Interval at which the AP attempts to connect to the WMI server. To configure this parameter, run the **keepalive interval** *interval* (WMI profile view) command.
Retry interval(min)	Interval at which the AP attempts to reconnect to the WMI server. To configure this parameter, run the **keepalive retry-interval** *retry-interval* (WMI profile view) command.
Retry number	Number of attempts the AP reconnects to the WMI server. To configure this parameter, run the **keepalive retry-number** *retry-number* (WMI profile view) command.
Device enable	Whether device monitoring data collection is enabled. To configure this parameter, run the **collect-item device-data disable** command.
Device data interval(s)	Interval at which device monitoring data is collected. To configure this parameter, run the **collect-item device-data interval** *interval* command.
Ssid enable	Whether SSID monitoring data collection is enabled. To configure this parameter, run the **collect-item ssid-data disable** command.
Ssid data interval(s)	Interval at which SSID monitoring data is collected. To configure this parameter, run the **collect-item ssid-data interval** *interval* command.
Radio enable	Whether radio monitoring data collection is enabled. To configure this parameter, run the **collect-item radio-data disable** command.

Item	Description
Radio data interval(s)	Interval at which radio monitoring data is collected. To configure this parameter, run the **collect-item radio-data interval** *interval* command.
Interface enable	Whether interface monitoring data collection is enabled. To configure this parameter, run the **collect-item interface-data disable** command.
Interface data interval(s)	Interval at which interface monitoring data is collected. To configure this parameter, run the **collect-item interface-data interval** *interval* command.
Terminal enable	Whether STA data collection is enabled. To configure this parameter, run the **collect-item terminal-data disable** command.
Terminal data interval(s)	Interval at which STA data is collected. To configure this parameter, run the **collect-item terminal-data interval** *interval* command.
Log enable	Whether log data collection is enabled. To configure this parameter, run the **collect-item log-data disable** command.
Log data interval(s)	Interval at which log data is collected. To configure this parameter, run the **collect-item log-data interval** *interval* command.
Location enable	Whether wireless device location data collection is enabled. To configure this parameter, run the **collect-item location-data enable** command.
Location data interval(s)	Interval at which wireless device location data is collected. To configure this parameter, run the **collect-item location-data interval** *interval* command.
Neighbor device enable	Whether surrounding radio data collection is enabled. To configure this parameter, run the **collect-item neighbor-device-data disable** command.
Neighbor device data interval(s)	Interval at which surrounding radio data is collected. To configure this parameter, run the **collect-item neighbor-device-data interval** *interval* command.
CP-CAR enable	Whether CPCAR data collection is enabled. To configure this parameter, run the **collect-item cpcar-data disable** command.

Item	Description
CP-CAR data interval(s)	Interval at which CPCAR data is collected. To configure this parameter, run the **collect-item cpcar-data interval** *interval* command.
EMDI enable	Whether eMDI data collection is enabled. To configure this parameter, run the **collect-item emdi-data disable** command.
EMDI data interval(s)	Interval at which eMDI data is collected. To configure this parameter, run the **collect-item emdi-data interval** *interval* command.
Application statistics enable	Whether site guest data collection is enabled. To configure this parameter, run the **collect-item application-statistics-data disable** command.
Application statistics data interval(s)	Interval at which site guest data is collected. To configure this parameter, run the **collect-item application-statistics-data interval** *interval* command.
Terminal DHCP option enable	Whether collection of DHCP Option information (Options 12, 55, and 60) in the DHCP packets sent by STAs is enabled. To configure this parameter, run the **collect-item terminal-dhcp-option-data enable** command.
Terminal DHCP option data interval(s)	Interval at which DHCP Option information (Options 12, 55, and 60) in the DHCP packets sent by STAs is collected. To configure this parameter, run the **collect-item terminal-dhcp-option-data interval** *interval* command.
Terminal HTTP UA enable	Whether collection of UA information in the HTTP packets sent by STAs is enabled. To configure this parameter, run the **collect-item terminal-http-ua-data enable** command.
Terminal HTTP UA data interval(s)	Interval at which UA information in the HTTP packets sent by STAs is collected. To configure this parameter, run the **collect-item terminal-http-ua-data interval** *interval* command.
Terminal mDNS enable	Whether collection of service information in the mDNS packets sent by STAs is enabled. To configure this parameter, run the **collect-item terminal-mdns-data enable** command.

Item	Description
Terminal mDNS data interval(s)	Interval at which service information in the mDNS packets sent by STAs is collected. To configure this parameter, run the **collect-item terminal-mdns-data interval** *interval* command.
DNS enable	Whether DNS data collection is enabled. To configure this parameter, run the **collect-item dns-data enable** command.
DNS data interval(s)	Interval at which DNS data is collected. To configure this parameter, run the **collect-item dns-data interval** *interval* command.
Non WiFi data enable	Whether collection of non-Wi-Fi device data is enabled. To configure this parameter, run the **collect-item non-wifi-data enable** command.
Non WiFi data interval(s)	Interval at which non-Wi-Fi device data is collected. To configure this parameter, run the **collect-item non-wifi-data interval** *interval* command.
Log module ID	ID of the module whose logs are to be reported. To configure this parameter, run the **ap log module mid** *mid* [**name** *name*] command.
S-ipfpm enable	Whether iPCA 2.0 measurement information collection is enabled. To configure this parameter, run the **collect-item s-ipfpm-data disable** command.
AI roam data enable	Whether AI roaming data collection is enabled. To configure this parameter, run the **collect-item ai-roam-data disable** command.
AI roam data interval(s)	Interval at which AI roaming data is collected. To configure this parameter, run the **collect-item ai-roam-data interval** *interval* command.
Lldp enable	Whether LLDP neighbor data collection is enabled. To configure this parameter, run the **collect-item lldp-data disable** command.
PKI realm	PKI realm used for interconnection with a WMI server. To configure this parameter, run the **pki realm** *realm-name* command.
Spectrum data enable	Whether spectrum analysis data collection is enabled. To configure this parameter, run the **collect-item spectrum-data enable** command.

11.20.8 keepalive (WMI profile view)

Function

The **keepalive** command configures connection parameters between APs and the WMI server.

The **undo keepalive** command restores the default settings of connection parameters between APs and the WMI server.

By default, the heartbeat interval is 3 minutes, the reconnection interval is 5 minutes, and the number of reconnection attempts is 0.

Format

keepalive { **interval** *interval* | **retry-interval** *retry-interval* | **retry-number** *retry-number* } *

undo keepalive

Parameters

Parameter	Description	Value
interval *interval*	Specifies the heartbeat interval.	The value is an integer that ranges from 1 to 60, in minutes.
retry-interval *retry-interval*	Specifies the reconnection interval after an AP is disconnected from the server.	The value is an integer that ranges from 5 to 60, in minutes.
retry-number *retry-number*	Specifies the number of reconnection attempts.	The value is an integer that ranges from 0 to 4294967295. The value 0 indicates that the server and APs always attempt to reconnect to each other.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number of reconnection attempts to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] keepalive retry-number 5
```

11.20.9 max-packet-size (WMI profile view)

Function

The **max-packet-size** command configures the maximum data length of KPI information sent by APs to a WMI server.

The **undo max-packet-size** command restores the default maximum data length of KPI information sent by APs to a WMI server.

By default, the maximum data length of KPI information sent by APs to a WMI server is 5 KB.

Format

max-packet-size *size*

undo max-packet-size

Parameters

Parameter	Description	Value
size	Specifies the maximum data length of reported information.	The value is an integer that ranges from 4 to 256, in KB.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

Based on the network status, you can run the **max-packet-size** command to configure the maximum data length of KPI information sent by APs to a WMI server.

Example

Set the maximum data length of KPI information sent by APs to a WMI server to 6 KB.

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



```
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] max-packet-size 6
```

11.20.10 mdns-snooping enable

Function

The **mdns-snooping enable** command enables the mDNS snooping function.

The **undo mdns-snooping enable** command disables the mDNS snooping function.

By default, mDNS snooping is disabled.

Format

mdns-snooping enable

undo mdns-snooping enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

In terminal type identification scenarios, you can enable mDNS snooping on a VAP. In this manner, the device can collect information from mDNS packets sent by terminals connected to the VAP and report the collected information to a WMI server for terminal type identification.

Example

Enable mDNS snooping.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name abc
[HUAWEI-wlan-vap-prof-abc] mdns-snooping enable
```

11.20.11 pki realm (WMI profile view)

Function

The **pki realm** command configures a PKI realm for interconnection between APs and a WMI server.

The **undo pki realm** command restores the default PKI realm for interconnection between APs and a WMI server.

By default, the PKI realm for interconnection between APs and a WMI server is **default**.

Format

pki realm *realm-name*

undo pki realm

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The PKI realm name must exist.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure a PKI realm for interconnection between APs and a WMI server.

Example

Configure the PKI realm **test** for interconnection between APs and a WMI server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wmi-server] pki realm test
```

11.20.12 report-interval (WMI profile view)

Function

The **report-interval** command sets the interval for APs to report KPI information to a WMI server.

The **undo report-interval** command restores the default interval for APs to report KPI information to a WMI server.

By default, APs report KPI information to a WMI server at an interval of 60 seconds.

Format

report-interval *interval*

undo report-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for APs to report KPI information to a WMI server.	The value is an integer that ranges from 10 to 300, in seconds.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

You can configure the interval for APs to report KPI information to a WMI server based on the device usage, network resource usage, and the server's requirements for real-time information collection. A shorter interval indicates that data is more frequently data, which occupies more device and network resources. A long interval cannot ensure real-time information on the server.

Example

Set the interval for APs to report KPI information to a WMI server to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] report-interval 30
```

11.20.13 server (WMI profile view)

Function

The **server** command configures the destination address and port number of the primary WMI server to which APs report KPI information.

The **undo server** command restores the default destination address and port number of the primary WMI server to which APs report KPI information.

By default, the destination address and port number of the primary WMI server to which APs report KPI information are not configured.

Format

server ip-address *ip-address* **port** *port*

undo server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address of the server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of the server.	The value is an integer that ranges from 1 to 65535. • Use port 10032 to report data to iMaster NCE-Campus. • Use port 27371 to report data to iMaster NCE-CampusInsight.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you configure a correct IP address and port number of a WMI server, APs can correctly report KPI information to the specified server.

NOTE

DNS information can be reported from APs only to iMaster NCE-CampusInsight.

Precautions

When the primary/backup WMI server scheme is used, run the **server backup ip-address** *ip-address* **port** *port* (WMI profile view) command to configure the destination address and port number of the backup WMI server after configuring the primary WMI server. If the primary/backup WMI server scheme is not used, you only need to configure the destination address and port number of the primary WMI server. Do not configure the backup server before configuring the primary server.

If the backup WMI server has been configured and you run the **undo server** command to restore the primary WMI server to the default value, the backup WMI server is also restored to the default value.

Example

Configure the destination IP address and port number for APs to report KPI information.

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



```
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] server ip-address 10.10.11.11 port 10032
```

11.20.14 server backup (WMI profile view)

Function

The **server backup** command configures the destination IP address and port number of the backup WMI server to which APs report KPI information.

The **undo server backup** command restores the default destination IP address and port number of the backup WMI server to which APs report KPI information.

By default, the destination IP address and port number of the backup WMI server to which APs report KPI information are not configured.

Format

server backup ip-address *ip-address* **port** *port*

undo server backup ip-address

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address of the server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of the server.	The value is an integer that ranges from 1 to 65535. • Use port 10032 to report data to iMaster NCE-Campus. • Use port 27371 to report data to iMaster NCE-CampusInsight.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the primary/backup WMI server scheme is used, you can run this command to configure the destination IP address and port number of the backup WMI server so that the APs can report KPI information to the specified backup WMI server.

After the primary/backup scheme is configured, if an AP fails to connect to the primary WMI server, the AP attempts to connect to the backup WMI server. If the connection still fails, the AP attempts to reconnect to the primary and backup WMI servers until the connection is successful.

NOTE

DNS information can be reported from APs only to iMaster NCE-CampusInsight.

Precautions

The destination IP address and port number of the primary WMI server have been configured using the **server ip-address** *ip-address* **port** *port* (WMI profile view) command.

Example

Configure the destination IP address and port number of the backup WMI server to which APs report KPI information.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] server ip-address 10.10.11.11 port 10032
[HUAWEI-wlan-wmi-server-prof-abc] server backup ip-address 10.10.11.12 port 10032
```

11.20.15 wmi-server (AP system profile view)

Function

The **wmi-server** command binds a WMI profile to the AP system profile.

The **undo wmi-server** command unbinds a WMI profile from the AP system profile.

By default, no WMI profile is bound to an AP system profile.

Format

wmi-server *profile-name* **index** *index*

undo wmi-server index *index*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WMI profile.	The WMI profile name must exist.

Parameter	Description	Value
index *index*	Specifies an index.	The value is an integer that can be 1 or 2. **NOTE** To report KPI information to iMaster NCE-Campus, specify index 1. To report KPI information to iMaster NCE-CampusInsight, specify index 2.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

A WMI profile can take effect only after being bound to an AP system profile.

NOTE

Do not bind two WMI profiles with the same destination address and port number to avoid waste of destination server resources.

Example

Bind WMI profile **abc** to the AP system view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys
[HUAWEI-wlan-ap-system-prof-apsys] wmi-server abc index 1
```

11.20.16 wmi-server (WLAN view)

Function

The **wmi-server** command creates a WMI profile and displays the WMI profile view.

The **undo wmi-server** command deletes a WMI profile.

By default, no WMI profile is created.

Format

wmi-server name *profile-name*

undo wmi-server { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WMI profile.	The value is a string of 1 to 35 case-insensitive characters, without spaces or quotation marks (?). It cannot start or end with double quotation masks (").
all	Specifies all WMI profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can set parameters for APs to report KPI information to the WMI server in the WMI profile.

Example

Create a WMI profile **abc** and display the WMI profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc]
```

11.21 Configuration Commands for the Zero-Roaming Distributed Wi-Fi Solution

11.21.1 display ap oru status

Function

The **display ap oru status** command displays the status of ORUs and AUs connected to DAPs.

NOTE

ORU management is supported only by the DAP AirEngine 9700D-S.

Format

display ap oru status { **all** | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Displays the status of ORUs and AUs connected to all DAPs.	-
ap-id *ap-id*	Displays the status of ORUs and AUs connected to a specified DAP.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to query the IDs, status, and versions of ORUs and AUs connected to a specified DAP or all DAPs.

Example

Display the status of ORUs and AUs connected to all DAPs.

```
<HUAWEI> display ap oru status all
Y: Normal N: Absent A: Abnormal U: Upgrading D: Disabled -: Unknown
ORUx: ORUx status(AU0 status/AU1 status/AU2 status/AU3 status/AU4 status/AU5 status/AU6 status/AU7
status)
-------------------------------------------------------------------------------------------------------------------
-----------------------------------
AP ID   ORU0            ORU1            ORU2            ORU3            ORU4            ORU5
ORU6            ORU7
-------------------------------------------------------------------------------------------------------------------
-----------------------------------
5       N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N) Y(Y/Y/N/N/N/N/N/N)
N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N)
-------------------------------------------------------------------------------------------------------------------
-----------------------------------
```

Table 11-318 Description of the **display ap oru status all** command output

Item	Description
AP ID	AP ID.

Item	Description
ORUx	Status of ORU*x* and its connected AUs. The possible status of an ORU includes: ● Y: Normal ● N: Absent ● A: Abnormal ● U: Upgrading ● D: Disabled ● -: Unknown The possible status of an AU includes: ● Y: Normal ● N: Absent ● -: Unknown

Display the status of ORUs and AUs connected to the DAP with the ID of 1.

```
<HUAWEI> display ap oru status ap-id 1
Y: Normal N: Absent -: Unknown
--------------------------------------------------------------------------------
ORU  SN          Status    AU status            Temperature(degree C)  Version
--------------------------------------------------------------------------------
0    XXX         Absent    N/N/N/N/N/N/N/N      -                      0
1    XXX         Absent    N/N/N/N/N/N/N/N      -                      0
2    XXX         Absent    N/N/N/N/N/N/N/N      -                      0
3    XXX         Normal    Y/Y/N/N/N/N/N/N      35                      7
4    XXX         Absent    N/N/N/N/N/N/N/N      -                      0
5    XXX         Absent    N/N/N/N/N/N/N/N      -                      0
6    XXX         Absent    N/N/N/N/N/N/N/N      -                      0
7    XXX         Absent    N/N/N/N/N/N/N/N      -                      0
--------------------------------------------------------------------------------
Total: 8
```

Table 11-319 Description of the **display ap oru status ap-id** command output

Item	Description
ORU	ORU ID.
SN	ORU SN.
Status	ORU status.
AU status	AU status.
Temperature(degree C)	ORU temperature. When the ORU state is **Absent** or **Disabled**, the temperature is displayed as a hyphen (-).
Version	Version number of the ORU.

11.21.2 distribute-mode enable

Function

The **distribute-mode enable** command enables the DAP network collaboration function.

The **undo distribute-mode enable** command restores the default state of the DAP network collaboration function.

By default, the DAP network collaboration function is disabled.

NOTE

Network collaboration functions (including intranet and extranet collaboration, and DAP backup) are supported only by the AirEngine 6761-21E with external antennas.

Format

distribute-mode enable

undo distribute-mode enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

This command is used to enable the DAP network coordination function. After an extranet AP or backup AP is connected to a DAP, you can run this command to enable the distributed AP network collaboration function. In this way, the extranet AP or backup AP can share the ORUs and AUs connected to the DAP, thereby achieving the backup solution or the integrated deployment of the intranet and extranet within the same coverage area.

Precautions

When configuring a backup solution, you also need to run the **type service-backup distribute** command to set the VAP type of the backup AP to distributed-AP backup service.

Example

Enable the DAP network collaboration function.

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



```
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] distribute-mode enable
```

11.21.3 oru reboot

Function

The **oru reboot** command restarts ORUs.

NOTE

ORU management is supported only by the DAP AirEngine 9700D-S.

Format

oru reboot ap-id *ap-id* [**oru-id** *oru-id*]

Parameters

Parameter	Description	Value
ap-id *ap-id*	Restarts the ORUs connected to a DAP with a specified ID.	The AP ID must exist.
oru-id *oru-id*	Restarts the ORU with a specified ID. If this parameter is not specified, all ORUs connected to the specified DAP are restarted.	The value is an integer that ranges from 0 to 7.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

When maintaining ORUs, you can run this command to restart ORUs as required.

Example

Restart the ORU connected to the DAP with the ID of 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] oru reboot ap-id 1
```


11.21.4 fastpass users

Function

The **fastpass users** command configures the FastPass function for VIP users on a DAP.

The **undo fastpass** command restores the default status of the FastPass function for VIP users on a DAP.

By default, the FastPass function for VIP users is enabled on the 2.4 GHz radio, the number of FastPass users is 5, the FastPass scheduling period is 20 ms, and the percentage of FastPass users in the scheduling period is 25%.

NOTE

The VIP FastPass function is supported only by the DAP AirEngine 9700D-S.

The FastPass function for VIP users applies only to the 2.4 GHz frequency band, and does not take effect after the configuration is delivered in the 5G radio profile view.

Format

fastpass users *value* [**period** *period-value* **ratio** *ratio-value*]

undo fastpass

Parameters

Parameter	Description	Value
value	Specifies the number of FastPass users.	The value is an integer that ranges from 0 to 10. When this parameter is set to 0, this function is disabled. The default value is 5.
period *period-value*	Specifies the FastPass scheduling period.	The value is of enumerated type, which can be 20, 40, 60, 80, or 100, in milliseconds. The default value is 20.
ratio *ratio-value*	Specifies the percentage of FastPass users in the scheduling period.	The value is an integer that ranges from 5 to 75, in percentage. The default value is 25.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In a zero-roaming distributed scenario, when the 2.4 GHz frequency band experiences severe interference and the channel utilization exceeds 60%, you can configure the FastPass function for VIP users to prevent packet loss and frame freezing, thereby preferentially ensuring user experience of important intranet services.

When the number of FastPass users specified by the parameter *value* is set to 0, this function is disabled.

When the channel utilization exceeds 60%, you are advised to set the number of FastPass users to 10, the FastPass scheduling period to 60 ms, and the percentage of FastPass users to 75%.

Example

Set the number of FastPass users to 10, the FastPass scheduling period to 60 ms, and the percentage of FastPass users in the scheduling period to 75%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] fastpass users 10 period 60 ratio 75
```

