11 WLAN-AC Commands

About This Chapter

11.1 WLAN Service Configuration Commands

11.1.1 Command Support

Only the S5720HI supports WLAN-AC commands.

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
```

Related Topics

11.1.86 display ac global configuration

11.1.3 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
```

11.1.4 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 MAC addresses of the STA, AP, and AC, AP name and current time, AC name and 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
```

11.1.5 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 configure an AC IPv4 address list for APs. After this list is configured, the APs can unicast a Discovery Request packet to discover an AC when they go online using IPv4 addresses.

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 provisioning 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
```

11.1.6 ac-list(AP provisioning 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 provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure an AC IPv4 address list for APs. After this list is configured, the APs can unicast a Discovery Request packet to discover an AC when they go online using IPv4 addresses.

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 AP provisioning view.

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

```
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] ac-list 192.168.10.1
```

Related Topics

11.1.73 commit (AP provisioning view)

11.1.128 display provision-ap parameter-list

11.1.7 active-dull-client enable

Function

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

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

By default, the function of preventing terminals from entering energy-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 energy-saving mode. You can run the **active-dull-client enable** command to enable the function of preventing terminals from entering energy-saving mode. After that, an AP frequently sends null data frames to these terminals to prevent them from entering energy-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 enters an abnormal energy-saving state, you are advised to disable the function.

Example

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

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

Related Topics

11.1.143 display ssid-profile

11.1.8 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, static, or SLAAC 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
```

Related Topics

11.1.73 commit (AP provisioning view)

11.1.128 display provision-ap parameter-list

11.1.9 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 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 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, 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
```

Related Topics

11.1.73 commit (AP provisioning view)

11.1.128 display provision-ap parameter-list

11.1.10 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
```

Related Topics

11.1.143 display ssid-profile

11.1.11 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.

NOTE

Only the AP8130DN support this function.

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 an AP8130DN or AP8130DN-W is deployed to provide 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.12 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 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.13 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.14 antenna-gain

Function

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

(AP group radio view) The **undo antenna-gain** command restores the default antenna gain for all specified 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 cancels the configuration of the antenna gain on an AP radio. The antenna gain on the AP radio is then determined by that configured in the AP group radio view.

By default, no antenna gain is configured for AP radios.

The antenna gain of AP radios depends on AP types and working channels of AP radios. You can run the **display ap-type** { **id** *type-id* | **type** *ap-type* } command to check default antenna gains of radios of different AP types.

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 0 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. In the same condition, if the antenna gain is high, the wave travels far.

Precautions

- The antenna gain of an AP radio configured using the command must be consistent with the gain of the antenna connected to the AP.
- The antenna gain of an AP radio configured using the command takes effect only for external antennas. When an AP uses an external antenna, configure the antenna gain for the AP radio to be consistent with the gain of the external antenna connected to the AP.
- The maximum antenna gain should comply with laws and regulations of the corresponding country. For details, see the *Country Code & Channel Compliance Table*. You can obtain this table at Huawei technical support website.
  - Enterprise technical support website: **http://support.huawei.com/enterprise**
  - Carrier technical support website: **http://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 5G antenna gain of an AP2010DN is 2.5 dB, the 5G antenna gain of 3 dB is displayed on the AC.

Example

# Set the antenna gain to 4 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] antenna-gain 4
```

11.1.15 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.

The default AP authentication mode is MAC address 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 non-authentication mode.	-
sn-auth	Indicates the SN authentication mode.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After the **ap auth-mode** command is executed, the AC authenticates the AP using the configured mode.

NOTE

The non-authentication mode brings security risks. You are advised to set the authentication mode to MAC address authentication or SN authentication, which is more secure.

Example

# Change the AP authentication mode to MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap auth-mode mac-auth
```

Related Topics

11.1.95 display ap global configuration

11.1.16 ap blacklist

Function

The **ap blacklist** command adds an AP to an AP blacklist.

The **undo ap blacklist** command deletes an AP from an AP blacklist.

By default, no AP is in an AP blacklist.

Format

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

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

Parameters

Parameter	Description	Value
mac *ap-mac1*	Specifies the AP MAC address.	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. This parameter is used when you want to add multiple MAC addresses to the blacklist. The value must be larger than *ap-mac1*. *ap-mac1* and *ap-mac2* identify a range. The maximum number of MAC addresses that can be added to the blacklist in batches is 128.	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

If the AP's MAC address is in the blacklist, the AP cannot go online. If the MAC address of an online AP is in the blacklist, the AP is forced to log out.

Precautions

The AP blacklist and whitelist can be configured at the same time. However, the MAC address of an AP cannot be added to the AP blacklist and whitelist at the same time.

If AP whitelist and blacklist are all configured, check whether an AP is on the blacklist first.

Example

# Add the AP with the MAC address of 0025-9e07-8280 to the AP blacklist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap blacklist mac 0025-9e07-8280
```

# Add MAC addresses from 0025-9e07-8270 to 0025-9e07-8276 to the AP blacklist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap blacklist mac 0025-9e07-8270 to 0025-9e07-8276
```

Related Topics

11.1.35 ap-confirm

11.1.90 display ap blacklist

11.1.17 ap data-collection enable

Function

The **ap data-collection enable** command enables an AC to buffer AP data.

The **undo ap data-collection enable** command restores the default settings.

By default, an AC is disabled from buffering AP data.

Format

ap data-collection enable

undo ap data-collection enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

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 buffer obtained data. Upon next data query, the AC can directly search for data in the buffer but does not 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 users on the AC, this function may occupy many memory resources and affect performance. Therefore, you are advised to disable this function when statistics query is not required.

After the **undo ap data-collection enable** command is executed, the AC stops periodically obtaining data from APs. Historical data in the buffer is not updated. To query latest statistics, enable this function again.

Example

# Enable an AC to buffer AP data.

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

Related Topics

11.1.18 ap data-collection interval

11.1.95 display ap global configuration

11.1.18 ap data-collection interval

Function

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

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

By default, an AC 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 the **ap data-collection interval** command to set the buffer duration.

Example

# Enable an AC 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
```

Related Topics

11.1.17 ap data-collection enable

11.1.95 display ap global configuration

11.1.19 ap lldp enable

Function

The **ap lldp enable** command enables 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

The Link Layer Discovery Protocol (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
```

Related Topics

11.1.95 display ap global configuration

11.1.183 lldp enable

11.1.20 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, factory settings of which need to be restored.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP, factory settings of which need to be restored.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP, factory settings of which 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 the AP, you can run this command to clear AP configurations.

NOTICE

After restoring factory settings, the AP is reset and configurations are restored to factory settings.

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
```

11.1.21 ap modify

Function

The **ap modify** command changes the MAC address of 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 change the MAC address of the AP to that of a new AP to prevent repetitive data configurations. After the change, the new AP goes online using the ID of the original AP, and all data configurations of the original AP take effect on the new AP.

By default, you can run the **display ap** { **all** | **ap-group** *ap-group* } command to check the MAC address of an AP.

Precautions

Replacing an AP enables the new AP to go online on the AC but will interrupt services of the original AP.

Example

# Replace the AP with the ID **0** with the AP with the MAC address **0002-1110-0120**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap modify 0 mac 0002-1110-0120
Warning: Modify AP will influence the service that has published in AP, Whether to continue? [Y/N]y
```

Related Topics

11.1.87 display ap

11.1.22 ap update ftp-server

Function

The **ap update ftp-server** command configures basic FTP information, including the FTP server IP address, FTP server user name and password.

The **undo ap update ftp-server** command restores default FTP settings.

By default, no IP address of the FTP server is configured, and the user name and password on the FTP server both have default settings. 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

ap update ftp-server ip-address *server-ip-address* **ftp-username** *ftp-username* **ftp-password cipher** *ftp-password*

undo ap update ftp-server

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies an IPv4 address for the FTP server.	The value is in dotted decimal notation.
ftp-username *ftp-username*	Specifies the FTP server user name.	The value is a string of 1 to 31 characters. The value 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 cipher text.	-

Parameter	Description	Value
ftp-password	Specifies the FTP server password.	The value is a string of characters without question marks (?). It cannot start or end with double quotation marks (" ") or spaces. *ftp-password* contains 188 characters in cipher text, such as %^%#A<g;&zQR7P3TF+,[MxQ1X%4[2~Gb]Vp#(e<y:~)/%^%#. *ftp-password* also can be a string of 1 to 128 characters in plain text, such as **huawei123**.

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.

- The FTP server user name cannot contain 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, FTP upgrade fails.

Example

# Configure the FTP server IP address, FTP server user name and password.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update ftp-server ip-address 192.168.1.100 ftp-username admin ftp-password
cipher wlanadmin
```

Related Topics

11.1.25 ap update mode

11.1.26 ap update multi-load

11.1.112 display ap update configuration

11.1.23 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.

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
```

Related Topics

11.1.25 ap update mode

11.1.26 ap update multi-load

11.1.112 display ap update configuration

11.1.24 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 update 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 **fitap6x10xn_v200r007c10.bin**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update load ap-name N1-2 update-filename fitap6x10xn_v200r007c10.bin
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP
or SFTP upgrade mode is recomm
ended. Continue? [Y/N]:y
```

Related Topics

11.1.28 ap update reset

11.1.114 display ap update status

11.1.25 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 upgrade versions from the AC.	-
ftp-mode	Indicates the FTP mode. The AC delivers the FTP configuration to APs using the **11.1.22 ap update ftp-server** command, and APs download the upgrade version file from the FTP server.	-

Parameter	Description	Value
sftp-mode	Indicates the SFTP mode. The AC delivers the SFTP configuration to APs using the **11.1.29 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.
- Run the **ap update multi-load** command to upgrade the AP.

Example

# Set the AP upgrade mode to **sftp-mode**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update mode sftp-mode
```

Related Topics

11.1.112 display ap update configuration

11.1.26 ap update multi-load

Function

The **ap update multi-load** command upgrades APs of the same type in batches.

The **undo ap update multi-load** command cancels batch upgrade of APs with the same type.

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 255.
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 ap-type** *type-id* command cancels batch upgrade of APs with the same type. 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* 19 in batches online.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update multi-load ap-type 19
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP
or SFTP upgrade mode is recomm
ended. Continue? [Y/N]:y
```

# Upgrade all APs in AP group **ap-group1** in batches online.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update multi-load ap-group ap-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 recomm
ended. Continue? [Y/N]:y
```

Related Topics

11.1.31 ap update update-filename

11.1.27 ap update multi-reset

11.1.114 display ap update status

11.1.27 ap update multi-reset

Function

The **ap update multi-reset** command resets APs in batches.

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>]

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 APs with the specified AP name.	The AP name must exist.
ap-id *ap-id*	Resets APs with the specified AP ID.	The AP ID must exist.

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.

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*, or **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* and **ap-id** *ap-id* are in different AP groups, the APs cannot be reset.

Example

# Reset APs with **type-id** 19 in batches.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update multi-reset ap-type 19
```

11.1.28 ap update reset

Function

The **ap update reset** command restarts a specified AP.

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 a single AP has been upgraded, run the **ap update reset** command to restart the AP and make the AP upgrade take effect.

Prerequisites

The AP is in normal or vmiss state.

The specified AP has been upgraded using the **ap update load** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } **update-filename** *update-file-name* command.

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 huawei.bin
[HUAWEI-wlan-view] ap update reset ap-name N1-2
```

Related Topics

11.1.24 ap update load

11.1.29 ap update sftp-server

Function

The **ap update sftp-server** command configures basic sftp information, including the sftp server IP address, sftp server user name and password.

The **undo ap update sftp-server** command restores default sftp settings.

By default, no IP address of the SFTP server is configured, and the user name and password on the SFTP server both have default settings. 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

ap update sftp-server ip-address *server-ip-address* **sftp-username** *sftp-username* **sftp-password cipher** *sftp-password*

undo ap update sftp-server

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies an IPv4 address for the sftp server.	The value is in dotted decimal notation.

Parameter	Description	Value
sftp-username *sftp-username*	Specifies the sftp server user name.	The value is a string of 1 to 31 characters. The value 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 cipher text.	-
sftp-password	Specifies the sftp server password.	The value is a string of characters without question marks (?). It cannot start or end with double quotation marks (" ") or spaces. *sftp-password* can be up to 188 characters in cipher text, such as %^%#A<g;&zQR7P3TF+,[MxQ1X%4[2~Gb]Vp#(e<y:~)/%^%#. *sftp-password* also can be a string of 1 to 128 characters in plain text, such as **huawei123**.

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.
- APs do not support the following characters:". Ensure that the sftp server user name and unencrypted password configured on the AC do not contain the preceding characters. Otherwise, sftp upgrade fails.

Example

# Configure the sftp server IP address, sftp server user name and password.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update sftp-server ip-address 192.168.1.100 sftp-username admin sftp-password cipher wlanadmin
```

Related Topics

11.1.25 ap update mode

11.1.26 ap update multi-load

11.1.112 display ap update configuration

11.1.30 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*.
- If an AC is used as the SFTP 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 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.

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
```

Related Topics

11.1.25 ap update mode

11.1.26 ap update multi-load

11.1.112 display ap update configuration

11.1.31 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 255.
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 the extension .bin.
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.

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 19 to **fitap6x10xn_v200r007c10.bin**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update update-filename fitap6x10xn_v200r007c10.bin ap-type 19
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
```

Related Topics

11.1.26 ap update multi-load

11.1.32 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.
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 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 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. To check the status of scheduled AP upgrade tasks, run the **display ap update schedule-task** command.

Configuration Impact

- 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.

Example

# Configure APs with **ap-type** as **54** to perform the scheduled upgrade from 01:00 to 04:00 on May 20, 2016.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update schedule-task task-id 1 start-time 1:00 2016/5/20 stop-time 4:00
2016/5/20 ap-type 54
```

Related Topics

11.1.31 ap update update-filename

11.1.113 display ap update schedule-task

11.1.33 ap username

Function

The **ap username** command sets the user name and password for AP login.

The **undo ap username** command restores the default user name and password for AP login.

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

ap username *username* **password cipher**

undo ap username

Parameters

Parameter	Description	Value
username	Specifies the user name for AP login.	The value is a string of 4-31 characters. It can contain letters, underlines, and digits. The character string must start with letters.
password	Specifies the password for AP login.	-

Parameter	Description	Value
cipher	Indicates the cipher text password.	The password can be entered in plain or cipher text: ● In plain text, the password is a string of 8 to 128 case-sensitive characters. It must contain at least one uppercase letter, one lowercase letter, and one digit except the question mark (?). ● In cipher text, the password is a string of 48 to 188 characters. It must contain at least one uppercase letter, one lowercase letter, and one digit.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Unauthorized users may use the default user name and password to log in to APs, causing security risk to APs. You can use the **ap username** command to change the user name and password to improve security for APs.

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 **huawei** and password to **Zz123456**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap username huawei password cipher
Enter the password (plain-text password of 8-32 characters or cipher-text passwo
rd of 48 or 68 characters):
Confirm password:
```

Related Topics

11.1.95 display ap global configuration

11.1.115 display ap username

11.1.34 ap whitelist

Function

The **ap whitelist** command adds an AP to an AP whitelist.

The **undo ap whitelist** command deletes an AP from an AP whitelist.

By default, no AP is in an 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*] | **sn** *ap-sn1* [**to** *ap-sn2*] }

Parameters

Parameter	Description	Value
mac *ap-mac1*	Specifies the AP MAC address.	The value is in H-H-H format. An H is a hexadecimal number of four digits.
to *ap-mac2*	Specifies the end MAC address. This parameter is used when you want to add multiple MAC addresses to the whitelist. The value must be larger than *ap-mac1*. *ap-mac1* and *ap-mac2* identify a range. The maximum number of MAC addresses that can be added to the whitelist in batches is 4096.	The value is in H-H-H format. An H is a hexadecimal number of four digits.
sn *ap-sn1*	Specifies the SN of an AP.	The value is a string of 1 to 31 characters.

Parameter	Description	Value
to *ap-sn2*	Specifies the end SN. This parameter is used when you want to add multiple SNs to the whitelist. It must be larger than *ap-sn1*. *ap-sn1* and *ap-sn2* identify a range. The maximum number of MAC addresses that can be added to the whitelist in batches is 4096.	The value is a string of 1 to 31 characters.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When the AP authentication mode is set to MAC address authentication using the **11.1.15 ap auth-mode** command, if the MAC address of an online AP exists in the whitelist, the AP is automatically added to the AC. If the MAC address of an online AP does not exist in the whitelist or the AP is not added offline, the AP cannot be automatically added to the AC. You need to run the **11.1.35 ap-confirm** command to confirm the AP.
- When the AP authentication mode is set to SN authentication using the **11.1.15 ap auth-mode** command, if the SN of an online AP exists in the whitelist, the AP is automatically added to the AC. If the SN of an online AP does not exist in the whitelist or the AP is not added offline, the AP cannot be automatically added to the AC. You need to run the **11.1.35 ap-confirm** command to confirm the AP.

Prerequisites

The AP authentication mode has been set to MAC address or SN authentication using the **11.1.15 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 AP MAC address 0025-9e07-8280 to the whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist mac 0025-9e07-8280
```

# Add the MAC addresses from 0025-9e07-8270 to 0025-9e07-8290 to the AP whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist mac 0025-9e07-8270 to 0025-9e07-8290
```

# Add 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
```

Related Topics

11.1.117 display ap whitelist

11.1.15 ap auth-mode

11.1.35 ap-confirm

11.1.35 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 hexadecimal number of four digits.
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 **11.1.110 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, added to the default region, and bound to the default AP profile.

Example

# Confirm the AP with MAC 0025-9e07-8270.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-confirm mac 0025-9e07-8270
```

# Confirm all APs.

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

Related Topics

11.1.87 display ap

11.1.117 display ap whitelist

11.1.95 display ap global configuration

11.1.36 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. It does not contain question marks (?), marks (/), or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all AP groups.	-

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 **11.1.38 ap-group (AP view)** or **11.1.46 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]
```

Related Topics

11.1.38 ap-group (AP view)

11.1.46 ap-regroup

11.1.119 display ap-group

11.1.37 ap-group (AP provisioning 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 the group that an AP joins.	The AP group must exist.

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the group that an AP joins is changed, and the change is delivered to the AP, the AP automatically restarts and joins the new group.

Follow-up Procedure

Run the **commit** command to deliver configuration to APs and restart the APs to make the configuration take effect.

Example

# Change the group that the AP joins to group **ap-new-group**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] ap-group ap-new-group
```

Related Topics

11.1.73 commit (AP provisioning view)

11.1.128 display provision-ap parameter-list

11.1.38 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 configuration
s of the radio, Whether to continue? [Y/N]:y
```

11.1.39 ap-id

Function

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

By default, no AP is added offline.

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 the AP ID.	The value is an integer that ranges from 0 to 1023.
type-id *type-id*	Specifies the AP type ID.	The value is an integer that ranges from 0 to 255.
ap-type *ap-type*	Specifies the 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 the serial number (SN) of an AP.	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

After an AP is successfully added to an AC, you can configure parameters for the AP offline. When the AP goes online, it uses the configured parameters.

You can run the **undo ap** command to delete an AP.

Precautions

To add an AP, you must enter the MAC address, SN, or MAC address+SN. 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

# Create an AP with ID **11**, type ID **19**, and MAC address **0025-9e07-8270**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 11 type-id 19 ap-mac 0025-9e07-8270
```

Related Topics

11.1.87 display ap

11.1.40 ap-mac

Function

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

By default, no AP is added offline.

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 the AP type ID.	The value is an integer that ranges from 0 to 255.
ap-type *ap-type*	Specifies the AP type.	The value is a string of 1 to 31 characters.
ap-id *ap-id*	Specifies the AP ID.	The value is an integer that ranges from 0 to 1023.
ap-sn *ap-sn*	Specifies the sequence number (SN) of an AP.	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

After an AP is successfully added to an AC, you can configure parameters for the AP offline. When the AP goes online, it uses the configured parameters.

Precautions

When adding an AP, you need to 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 entered 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

# Add the AP with the MAC address **0025-9e07-8260**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-mac 0025-9e07-8260
```

Related Topics

11.1.87 display ap

11.1.41 ap-mode

Function

The **ap-mode** command sets the working mode of an AP.

The **undo ap-mode** command restores the default working mode of an AP.

By default, an AP works in Fit mode.

Format

ap-mode { **fat** | **cloud** }

undo ap-mode

Parameters

Parameter	Description	Value
fat	Specifies the Fat mode.	-
cloud	Specifies the cloud 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 delivers 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.

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

Only the AP1050DN-S, AP2050DN, AP2050DN-E, AP4050DN-E, AP4050DN-HD, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP6050DN, AP6150DN, AP7050DN-E, AP7050DE, AP8030DN, AP8130DN, AD9430DN-12, and AD9430DN-24 support this command. The AP4030TN and AD9431DN-24X can be switched only to the Fat mode.

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
```

Related Topics

11.1.73 commit (AP provisioning view)

11.1.42 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]
```

Related Topics

11.1.87 display ap

11.1.43 ap-name (AP provisioning view)

Function

The **ap-name** command sets the name of an AP.

The **undo ap-name** command restores the default name of an AP.

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 31 case-sensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

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 automatically restarts and 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
```

Related Topics

11.1.73 commit (AP provisioning view)

11.1.128 display provision-ap parameter-list

11.1.44 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 31 case-sensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

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.

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
```

11.1.45 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
```

11.1.46 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.
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 **11.1.36 ap-group** command.

Configuration Impact

Changing the group of an AP will restart the AP and interrupt services. Exercise caution when you run the command.

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 1047-80b1-56a0 new-group group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and
antenna gain configuration
s of the radio, Whether to continue? [Y/N]:y
```

Related Topics

11.1.36 ap-group

11.1.87 display ap

11.1.47 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 31 case-sensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

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
```

Related Topics

11.1.87 display ap

11.1.48 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* } }

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 (,) 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-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.

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
```

11.1.49 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 **11.1.50 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]
```

Related Topics

11.1.50 ap-system-profile (AP group view and AP view)

11.1.120 display ap-system-profile

11.1.50 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 **11.1.49 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
```

Related Topics

11.1.36 ap-group

11.1.49 ap-system-profile (WLAN view)

11.1.132 display references ap-system-profile

11.1.51 assignment

Function

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

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

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

Format

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

undo assignment

Parameters

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

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

Precautions

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

Configuration Impact

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

Example

# Set the VLAN assignment algorithm to **even** in a VLAN pool.

```
<HUAWEI> system-view
[HUAWEI] vlan pool pool1
[HUAWEI-vlan-pool-pool1] assignment even
```

Related Topics

11.1.153 display vlan pool

11.1.289 vlan (VLAN pool view)

11.1.52 association-timeout

Function

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

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

By default, the association aging time 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 the **association-timeout** 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
```

Related Topics

11.1.143 display ssid-profile

11.1.53 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.

Parameter	Description	Value
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
```

Related Topics

11.1.150 display vap

11.1.245 service-mode disable

11.1.54 beacon-2g-rate

Function

The **beacon-2g-rate** command sets the transmit rate of 2.4 GHz Beacon frames.

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

By default, the transmit rate of 2.4 GHz Beacon frames is 1 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 Beacon frames.	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, WDS profile view, Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

Precautions

Modifying the transmit rate of Beacon frames will affect the association experience of STAs. Exercise caution when running the command.

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 Beacon 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 Mbps, 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 Beacon 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
```

Related Topics

11.1.143 display ssid-profile

11.1.223 radio-type (2G radio profile view)

11.1.55 beacon-5g-rate

Function

The **beacon-5g-rate** command sets the transmit rate of 5 GHz Beacon frames.

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

By default, the transmit rate of 5 GHz Beacon 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 Beacon frames.	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, WDS profile view, Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

Precautions

Modifying the transmit rate of Beacon frames will affect the association experience of STAs. Exercise caution when running the command.

Example

# Set the transmit rate of 5 GHz Beacon 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
```

Related Topics

11.1.143 display ssid-profile

11.1.56 beacon-interval

Function

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

The **undo beacon-interval** restores the default interval for sending 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 (except the AP7030DE and AP9330DN):

- 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

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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.57 beamforming enable

Function

The **beamforming enable** command enables Beamforming.

The **undo beamforming enable** command disables Beamforming.

By default, Beamforming is disabled.

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 signal-to-noise ratio (SNR) for the destination device.

Precautions

If nodes on the WDS or Mesh network are fixed and distant from each other, enable Beamforming to increase WDS or Mesh link SNR. Mobile nodes may cause low link SNR in WDS or Mesh scenarios. To prevent this problem, disable Beamforming. Among Beamforming-capable APs, the AP2x10xN series, AP7x30xE series, and AP9330DN APs do not support WDS and Mesh.

The smart antenna function cannot take effect if MU-MIMO has been configured.

Table 11-1 describes the support of Huawei APs for beamforming.

Table 11-1 Support of APs for Beamforming

AP Model	Explicit 802.11ac Beamforming	Explicit 802.11n Beamforming		Implicit Beamforming
		2.4 GHz	5 GHz	
AP3010DN, AP5010SN, AP5010DN, AP6010SN, AP6010DN, AP6310SN, AP6510DN, AP6610DN, AP7110SN, AP7110DN, and AP2010DN	N	Y	Y	N
AP5030DN, AP5130DN, AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP9131DN, AP9132DN, AD9430DN-12 (with R240D), AD9430DN-24 (with R230D and R240D), AD9431DN-24X (with R230D and R240D), and AP4030TN	N	Y For AP4030TN, only the radio 0 supports this feature.	N	N
AP8030DN, AP8130DN, AP1050DN-S, and AP8130DN-W	N	N	N	N

AP Model	Explicit 802.11ac Beamforming	Explicit 802.11n Beamforming		Implicit Beamforming
		2.4 GHz	5 GHz	
AD9430DN-12 (with R250D), AD9430DN-24 (with R250D, R450D and R250D-E), AD9431DN-24X (with R250D, R450D and R250D-E), AP2050DN, AP2050DN-E, AP4050DN-E, AP4050DN-HD, AP4051TN, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8150DN, AP8050DN-S, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP6050DN, AP6150DN, AP7050DN-E, and AP7050DE	Y	N	N	Y
AP7030DE and AP9330DN	N	N	N	Y

Example

# Enable Beamforming.

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

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.58 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.

By default, the 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	Indicates the priority of CAPWAP management packets from an AC to an AP. The priority of CAPWAP management packets determines the reliability of the link between an AC and an AP.	-
remote	Indicates the priority of CAPWAP management packets from an AP to an AC. The priority of CAPWAP management packets determines the reliability of the link between an AP and an 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 use the **capwap control-link-priority** command to configure the DSCP priority of CAPWAP management packets. A higher priority indicates a more reliable link between the AC and AP.

The configuration of the priority of CAPWAP management packets from an AC to an AP takes effect immediately. After the priority of CAPWAP management packets from an AP to an AC is changed, if the AP is online, the priority is sent 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 once the AP receives it.

Precautions

NOTICE

Configure priority 4 to 7 for CAPWAP management packets from an AC to an AP, preventing the CAPWAP management tunnel from being interrupted due to large traffic.

Example

# Set the priority of CAPWAP management packets from an AC to an AP to 6.

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

Related Topics

11.1.122 display capwap configuration

11.1.59 capwap dtls control-link encrypt

Function

The **capwap dtls control-link encrypt** command enables the function of encrypting the CAPWAP control tunnel using Datagram Transport Layer Security (DTLS).

The **undo capwap dtls control-link encrypt** command disables the function of encrypting the CAPWAP control tunnel using DTLS.

By default, the function of encrypting the CAPWAP control tunnel using DTLS 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 the AC, the AP obtains the AC IP address using the discovery mechanism. Then in the DTLS negotiation phase, the CAPWAP tunnel encrypts UDP packets using DTLS.

After this command is run, the CAPWAP control packets between the AP and AC are encrypted using DTLS, and the AP and AC use the PSK to perform DTLS negotiation. If the DTLS negotiation fails, the CAPWAP tunnel cannot be established.

Configuration Impact

After this command is run, the AP and AC reestablish a CAPWAP tunnel.

Precautions

When is enabled or APs are being upgraded, the status of DTLS encryption cannot be changed.

Example

# Enable the function of encrypting the CAPWAP control tunnel using DTLS.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls control-link encrypt
Warning: The DTLS PSK is the default one. It is recommended to change it to ensure security. Change it now?[Y/N]:y
New PSK:huawei@123
Configuring the new PSK, waiting......................done.
Warning: This operation may cause devices connected through CAPWAP to reset or go offline. Continue?[Y/N]:y
```

Related Topics

11.1.122 display capwap configuration

11.1.60 capwap dtls psk

Function

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

The **undo capwap dtls psk** command restores the default pre-shared key used for DTLS encryption.

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 dtls psk *psk-value*

undo capwap dtls psk

Parameters

Parameter	Description	Value
psk-value	Specifies the pre-shared key used for DTLS encryption.	The value is string of characters. The pre-shared key contains 48 or 68 characters in cipher text, for example, %^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#, or contains 6 to 32 characters in plain text, for example, a1234567. The password 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 a pre-shared key is used for DTLS encryption, you can use the **capwap dtls psk** command to change the pre-shared key.

NOTE

It is recommended that you change the pre-shared key in a timely manner to ensure device security.

Follow-up Procedure

Run the **capwap dtls control-link encrypt** command to enable CAPWAP control tunnel encapsulation using DTLS.

Precautions

After the **capwap dtls psk** command configuration is complete, the new pre-shared key will be automatically synchronized to the online APs that are working properly, but the previous pre-shared key still takes effect. The new pre-shared key takes effect after these APs go online again.

Example

# Configure the pre-shared key for DTLS encryption as **huawei123**.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls psk huawei123
```

Related Topics

11.1.59 capwap dtls control-link encrypt

11.1.61 capwap dtls psk-mandatory-match enable

11.1.122 display capwap configuration

11.1.61 capwap dtls psk-mandatory-match enable

Function

The **capwap dtls psk-mandatory-match enable** command enables an AP to establish a Datacom Transport Layer Security (DTLS) session with an AC using the default pre-shared key.

The **undo capwap dtls psk-mandatory-match enable** command disables an AP to establish a Datacom Transport Layer Security (DTLS) session with an AC using the default pre-shared key.

By default, an AP is disabled to establish a DTLS session with an AC using the default pre-shared key.

Format

capwap dtls psk-mandatory-match enable

undo capwap dtls psk-mandatory-match enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a new AP is added to the WLAN or the passwords of the AP and AC are different (for example, the password of the AC is changed but the AP is not online), you can enable the AP to perform DTLS sessions with the AC using the default pre-shared key. After three DTLS session failures, the AP notifies the AC of DTLS sessions using the default pre-shared key. In this way, a CAPWAP tunnel is established between the AP and the AC.

Example

# Enable the AP to establish a DTLS session with the AC using the default pre-shared key.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls psk-mandatory-match enable
```

Related Topics

11.1.122 display capwap configuration

11.1.62 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.

By default, If dual-link backup is enabled, the CAPWAP heartbeat detection interval is 25s and the number of CAPWAP heartbeat detections is 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, the interval at which two detection packets are sent.	The value is an integer ranging from 20 to 300, in seconds.

Parameter	Description	Value
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 ranging from 3 to 120.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined by CAPWAP, an AP and an AC send handshake packets periodically to maintain the data channel and management channel. If the AP does not receive packets from the AC within the heartbeat detection interval, it considers that the link between them is disconnected. Then the AP resets and releases its IP address, and reestablishes a link. If the AC does not receive packets from the AP within the heartbeat detection interval, it disconnects the link between the AC and the AP and reports an error message to the AP.

Precautions

If dual-link backup is enabled, the CAPWAP heartbeat detection interval is 25s and the number of CAPWAP heartbeat detections is 3. When the Wireless Distribution System (WDS) is required in dual-link backup configuration, the WDS link may be unstable and users may not access the network. You need to run this command to set the interval for CAPWAP heartbeat detection 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. 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
```

Related Topics

11.1.58 capwap control-link-priority

11.1.122 display capwap configuration

11.1.63 capwap echo-timeout trace logging

Function

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

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

By default, the Echo packet process trace and diagnosis 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 diagnosis logs are recorded upon AP Echo packet timeout.

Example

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

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

11.1.64 capwap message-integrity psk

Function

The **capwap message-integrity psk** command configures a pre-shared key (PSK) for checking integrity of CAPWAP packets.

The **undo capwap message-integrity psk** command restores the default PSK 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 for checking integrity of CAPWAP packets.	The value can be a string of 48 or 68 characters in cipher text (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#**) or a string of 6 to 32 characters in plain text (for example, **a1234567**). The key must contain at least two 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 pre-shared key 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 this configuration is complete, all online APs on the AC go offline.

Example

# Set the PSK for checking integrity of CAPWAP packets to **huawei@123**.

```
<HUAWEI> system-view
[HUAWEI] capwap message-integrity psk huawei@123
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
```

Related Topics

11.1.65 capwap message-integrity check disable

11.1.122 display capwap configuration

11.1.65 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 this 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
```

Related Topics

11.1.64 capwap message-integrity psk

11.1.122 display capwap configuration

11.1.66 capwap sensitive-info psk

Function

The **capwap sensitive-info psk** command modifies the pre-shared key (PSK) used for sensitive information encryption.

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

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 sensitive information encryption.	The value can be a string of 48 or 68 characters in cipher text (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#**) or a string of 6 to 32 characters in plain text (for example, **a1234567**). The key must contain at least two 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 transmitted 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 use the **capwap sensitive-info psk** command to modify the PSK used for sensitive information encryption.

NOTE

To ensure STA security, you are advised to modify the PSK value.

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

Precautions

In hot backup (HSB) and dual-link cold backup scenarios, the PSKs configured on the active and standby ACs must be the same. Otherwise, APs cannot set up CAPWAP tunnels with the standby AC.

The pre-shared key for encrypting sensitive information cannot be modified when an AP is being upgraded on the

Example

# Modify the PSK for encrypting sensitive information to **huawei@123**.

```
<HUAWEI> system-view
[HUAWEI] capwap sensitive-info psk huawei@123
Warning: This operation may cause devices using CAPWAP connections to go offline. Continue? [Y/N]:y
```

Related Topics

11.1.122 display capwap configuration

11.1.67 capwap source interface

Function

The **capwap source interface** command configures the source interface that the AC uses to establish a CAPWAP tunnel with an access device.

The **undo capwap source interface** command restores the source interface that the AC uses to establish a CAPWAP tunnel with an access device to the default setting.

By default, no source interface is configured for the AC to establish a CAPWAP tunnel with the access device.

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.

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.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AC uses the IP address of the specified interface as the source IP address. All access devices connected to the AC can learn this IP address and use the IP address to communicate with the AC.

Prerequisites

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

Precautions

A maximum of eight AC source interfaces can be configured.

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

Configure multiple source interfaces. When the source interfaces are added to different VPN instances, the IP addresses of these interfaces cannot be the same.

When multiple CAPWAP source interfaces are configured, ensure that the management VLAN for APs is within the VLAN range mapping the source interfaces. Otherwise, APs cannot go online.

Changing configuration of the CAPWAP source interface will clear statistics of the 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
```

Related Topics

11.1.122 display capwap configuration

11.1.68 channel

Function

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

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

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

(AP radio view) The **undo channel** command cancels the configuration of the working bandwidth and channel on an AP radio. The working bandwidth and channel on the AP radio are then determined by 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.

You can run the **11.1.91 display ap config-info** command to check the channel in use on a radio.

Format

channel { **20mhz** | **40mhz-minus** | **40mhz-plus** | **80mhz** | **160mhz** } *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.	-
80+80mhz	Sets the working bandwidth of a radio to 80+80 MHz.	-

Parameter	Description	Value
channel/ channel1/ channel2	Specifies the working channel for a radio. The channel is selected based on the country code and radio mode.	The parameter is an enumeration value. The value range is determined according to 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 configured channel parameters 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: **http://support.huawei.com/enterprise**
- Carrier technical support website: **http://support.huawei.com**

The channels you configure must be supported by the terminals; otherwise, the terminals cannot discover wireless 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 not detecting radar signals on it.

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

If an AP works in dual-5G mode, the channels of the two 5G radios must be separated by at least one channel.

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

NOTE

- The 80 MHz, 160 MHz, and 80+80 MHz working bandwidths are only supported in the 5G radio view.
- Currently, only the 5 GHz radio of the AP6050DN, AP6150DN, AP7050DE, and 7050DN-E supports 160 MHz, and 80+80 MHz. Only the 5 GHz radio of the AD9430DN-24 (including the mapping RUs), AD9430DN-12 (including the mapping RUs), AD9431DN-24X (including the mapping RUs), AP7030DE, AP9330DN, AP2030DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP3010DN-V2 (supporting 802.11ac after being upgraded from a version earlier than V200R008C10SPC300 to V200R008C10SPC300 or a later version), AP4030TN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DN-E, AP7050DE, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP1050DN-S, AP2050DN, AP2050DN-E, AP8130DN-W, AP5030DN, AP5130DN, AP8030DN, AP8130DN, AP4030DN, AP4130DN, AP9131DN, and AP9132DN supports 80 MHz.

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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.69 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 AP channel mode to outdoor mode.

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

The AP is automatically reset after this command is executed, so exercise caution when using this command.

These commands are supported by only the AP8030DN, AP8130DN, AP8050DN, AP8050DN-S, AP8150DN, AP8130DN-W, AP8050TN-HD, AP8082DN, and AP8182DN.

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: Modifying the channel set mode may delete channels of AP radios in this
 domain and restart the AP. Continue?[Y/N]:y
```

11.1.70 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 dynamic frequency selection (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.

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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.71 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.72 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
```

Related Topics

11.1.128 display provision-ap parameter-list

11.1.73 commit (AP provisioning view)

Function

The **commit** command commits configuration to an AP, a group of APs or all the on-line 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.
ap-group *ap-group-name*	Commits configuration to the AP in the specified AP group.	The AP group must already exist.

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 configuration to the AP with the MAC address **0023-0024-0080**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] commit ap-mac 0023-0024-0080
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
```

Related Topics

11.1.128 display provision-ap parameter-list

11.1.74 console disable

Function

The **console disable** command disables a user from logging in to the AP through a console interface.

The **undo console disable** command enables a user from logging in to the AP through a console interface.

By default, a user can log in to the AP through a console interface.

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 interface to manage and configure the AP.

After the **console disable** command is run, unauthorized users cannot log in to the AP through the console interface to perform operations.

Example

# Disable a user to log in to the AP through a console interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] console disable
```

Related Topics

11.1.120 display ap-system-profile

11.1.75 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.

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.
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.

Parameter	Description	Value
latitude s *latitude-value*	Specifies the south longitude 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 longitude 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
```

Related Topics

11.1.93 display ap coordinate

11.1.76 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

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 profile to be created, 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.

Example

# Create the VAP profile **huawei** and copy data from the profile **sample**.

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

```
[HUAWEI-wlan-view] vap-profile name huawei
[HUAWEI-wlan-vap-prof-huawei] copy-from sample
```

11.1.77 country-code

Function

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

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

By default, the country code **CN** is configured.

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

Country Code	Country/Region
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
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GE	Georgia
GR	Greece
GT	Guatemala

Country Code	Country/Region
HK	Hong Kong, Special Administrative Region of 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
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania
LU	Luxembourg
LV	Latvia
MA	Morocco
MC	Monaco
MK	Republic of North Macedonia
MO	Macao, Special Administrative Region of China
MT	Malta
MX	Mexico

Country Code	Country/Region
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
SV	El Salvador
SY	Syria
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad & Tobago
TW	Taiwan, Province of China
UA	Ukraine

Country Code	Country/Region
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 in different countries or regions, such as power requirements and channel requirements.

Configuration Impact

Modifying the country code in a regulatory domain profile will restart APs using the profile.

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 channel, power and antenna gain configurations of the
radio and reset the AP. Continu
e?[Y/N]:y
```

Related Topics

11.1.141 display regulatory-domain-profile

11.1.78 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 cancels the configuration of the radio coverage distance parameter on an AP radio. The radio coverage distance parameter on the AP radio is then determined by 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 distance parameter based on the AP distance. APs adjust the values of slottime, acktimeout, and ctstimeout values based on the distance parameter.	The value is an integer that ranges from 1 to 400, in 100 meters.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In actual application scenarios, two APs may be connected over dozens of meters to dozens of kilometers. Due to different AP distances, the time to wait for ACK packets from the peer AP varies. A proper acktimeout value can improve data transmission efficiency between APs.

You can configure the radio coverage distance parameter based on distances between APs and the APs automatically adjust the values of slottime, acktimeout, and ctstimeout based on the configured distance parameter 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 1.

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

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.79 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, the AP sends an alarm message to the AC, and the AC displays the alarm information.
- When the CPU usage of an AP falls below the alarm threshold, the AP sends a clear alarm message to the AC, and the AC displays the clear alarm information.

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
```

11.1.80 crc-alarm enable

Function

The **crc-alarm enable** command enables the alarm function for CRC errors on the AP 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 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 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 wired interface.	The value is an integer ranging 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*.

Parameter	Description	Value
low-threshold *low-threshold-value*	Specifies the clear alarm threshold for CRC errors on the AP wired interface.	The value is an integer ranging 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 **11.1.244 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
```

Related Topics

11.1.127 display port-link-profile

11.1.244 sample-time

11.1.81 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 ipv4 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.

The AP wired interfaces added to an Eth-trunk interface do 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
```

Related Topics

11.1.154 display wired-port-profile

11.1.82 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
```

Related Topics

11.1.143 display ssid-profile

11.1.83 description (AP wired port profile view)

Function

The **description** command configures the description of an AP wired port.

The **undo description** command restores the default description of an AP wired port.

By default, the port has no description.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the AP interface description.	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
```

Related Topics

11.1.154 display wired-port-profile

11.1.84 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
```

Related Topics

11.1.85 dhcp option82 format (vap profile view)

11.1.152 display vap-profile

11.1.85 dhcp option82 format (vap profile view)

Function

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

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

By default, the format of the Option 82 field inserted in DHCP packets sent by STAs is **ap-mac**.

Format

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

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

Parameters

Parameter	Description	Value
circuit-id	Specifies the circuit-ID (CID) in the Option 82 field.	-
remote-id	Specifies the remote-ID (RID) in the Option 82 field.	-
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.	-
user-defined *text*	Sets the format of Option 82 to the user-defined format.	The value is a string of 1 to 255 characters.

Parameter	Description	Value
ap-name	Specifies the AP name in the Option 82 field.	-
ap-name-ssid	Specifies the AP name and SSID in the Option 82 field.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

After an AP is enabled to insert the Option 82 field in DHCP packets sent from a STA, 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**: MAC address of the AP. After DHCP packets from a STA reach an AP, the AP inserts its MAC address into the Option 82 field of the DHCP packets.
- **ap-mac-ssid**: MAC address and SSID of the AP. After DHCP packets 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 packets.
- **ap-name**: AP name. After DHCP packets from a STA reach an AP, the AP inserts its name into the Option 82 field of the DHCP packets.
- **ap-name-ssid**: AP name and SSID. After DHCP packets from a STA reach an AP, the AP inserts its name and associated SSID into the Option 82 field of the DHCP packets.

If **mac-format** is not specified in the **dhcp option82** { **circuit-id** | **remote-id** } **format** { **ap-mac** | **ap-mac-ssid** } command, the AP 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 **remote-id** in Option 82 carried in DHCP packets sent by 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
```

Related Topics

11.1.84 dhcp option82 insert enable

11.1.152 display vap-profile

11.1.86 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 **11.1.2 ac sysnetid** command.

Related Topics

11.1.2 ac sysnetid

11.1.87 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 group to which an AP belongs.	The AP group must exist.
by-ssid *ssid*	Specifies an SSID.	The value must be an existing SSID.

Parameter	Description	Value
by-state *state*	Specifies the status of the AP.	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 first link is established. ● **name-conflicted**: Displays

Parameter	Description	Value
		information about APs having duplicate names. ● **normal**: Displays information about APs in normal state. ● **standby**: Displays information about APs in standby AC 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.

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]
Extra information:
P  : insufficient power supply
```

```
----------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP              Type            State STA Uptime      ExtraInfo
----------------------------------------------------------------------------------------------
0    dcd2-fcf6-76a0 area_1  ap-group1 192.168.120.254 AP6010DN-AGN     nor   0   4H:49M:11S  P
1    60de-4474-9640 area_2 ap-group1 192.168.120.253 AP5010DN-AGN     nor   0   6H:3M:40S   -
----------------------------------------------------------------------------------------------
Total: 2
```

# Display information about APs bound to SSID **hw-wlan**.

```
<HUAWEI> display ap by-ssid hw-wlan
Total AP information:
nor  : normal          [2]
Extra information:
P  : insufficient power supply
----------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP              Type            State STA Uptime      ExtraInfo
----------------------------------------------------------------------------------------------
0    dcd2-fcf6-76a0 area_1  ap-group1 192.168.120.254 AP6010DN-AGN     nor   0   4H:49M:11S  P
1    60de-4474-9640 area_2 ap-group1 192.168.120.253 AP5010DN-AGN     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]
Extra information:
P  : insufficient power supply
-------------------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP              Type            State          STA Uptime      ExtraInfo
-------------------------------------------------------------------------------------------------------
0    dcd2-fcf6-76a0 area_1  ap-group1 192.168.120.254 AP6010DN-AGN     normal          0   4H:50M:55S  P
1    60de-4474-9640 area_2 ap-group1 192.168.120.253 AP5010DN-AGN     normal          0   6H:5M:24S   -
-------------------------------------------------------------------------------------------------------
Total: 2
```

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

Item	Description
ID	AP ID.
MAC	MAC address of an AP.
Name	AP name.
Group	AP group.
IP	AP IP address.
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.
ExtraInfo	Extra information. The value **P** indicates that the power supply to an AP is insufficient.

Table 11-5 AP state list

AP State	Description	Possible Cause	Handling Suggestion
commit-failed	WLAN service configurations fail to be delivered to an AP after the AP goes online on an AC.	After the 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	WLAN service configurations are being delivered to an AP after the AP goes online on an AC.	After the AP goes online on the AC, WLAN service configurations are being delivered to the AP.	This is a normal state, and no action is required.
config	WLAN service configurations are being delivered to an AP when the AP is going online on an AC.	After the 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	WLAN service configurations fail to be delivered to an AP when the AP is going online on an AC.	After the 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.

AP State	Description	Possible Cause	Handling Suggestion
download	An AP is in upgrade state.	When the 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.	The 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.	Handle the AP online failure. For details, see **AP Online Failure** in the *Troubleshooting Insights*.

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.	The AP has not established a CAPWAP link with the AC, the MAC address and SN of the AP that is added offline are different from the actual ones, or license resources are insufficient.	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 obtain 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**

AP State	Description	Possible Cause	Handling Suggestion
			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 license resources of the AC.
name-conflicted	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	An AP is working properly.	An AP successfully goes online on an AC.	This is a normal state, and no action is required.
standby	The AP is in normal state on the standby AC.	In the HSB, dual-link cold backup, or N+1 backup scenario, if the link between the active and standby ACs is established properly, the AP is in standby state on the standby AC and in normal state on the active AC.	This is a normal state, and no action is required.

AP State	Description	Possible Cause	Handling Suggestion
ver-mismatch	The version of an AP does not match that of an AC on which the AP is to go online.	The versions of the AP and the AC mismatch.	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: **http://support.huawei.com/enterprise** ● Carrier technical support website: **http://support.huawei.com**
countryCode-mismatch	The country code of an AP does not match that of the AC on which the AP is about to go online.	The current version of the AP does not support the country code configured on the AC.	The AP does not support the country code. Upgrade the AP or change the country code configured on the AC.
unauthed	The AP is not authenticated.	The AP fails to be authenticated.	Run the **ap-confirm** command to confirm unauthenticated APs and allow them to go online.

Related Topics

11.1.39 ap-id

11.1.40 ap-mac

11.1.88 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 **huawei**.

```
<HUAWEI> display ap around-ssid-list ap-name huawei
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 11-6 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.

11.1.89 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
----------------------------------------------------------------------------
hw1     dcd2-fcf4-6600 2015-1-19 14:41:59      update
hw2     dcd2-fcf4-8800 2015-1-19 14:45:56      clear config
----------------------------------------------------------------------------
Total: 2
```

Table 11-7 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.

11.1.90 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 forced to log out.

Example

# Display the AP blacklist.

```
<HUAWEI> display ap blacklist
--------------------------------------------------------------------------------
ID     MAC
--------------------------------------------------------------------------------
0      0001-0002-0001
--------------------------------------------------------------------------------
Total: 1
```

Table 11-8 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 add MAC addresses to the AP blacklist, run the **11.1.16 ap blacklist** command.

Related Topics

11.1.16 ap blacklist

11.1.91 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.
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 AP **huawei**.

```
<HUAWEI> display ap config-info ap-name huawei
--------------------------------------------------------------------------------
AP MAC                          : dcd2-fcf6-76a0
AP SN                           : 210235419610D2000097
AP type                         : AP6010DN-AGN
AP name                         : huawei
AP group                        : default
Country code                    : CN
--------------------------------------------------------------------------------
Radio 0 configurations:
 Radio enable                   : yes
 Work mode                      : normal
 WDS  mode                      : -
 Mesh mode                      : -
 Radio band                     : 2.4G
 Radio type                     : bgn
 Config channel/bandwidth       : -/20M
 Actual channel/bandwidth       : 1/20M
 Config EIRP                    : 127
 Actual EIRP                    : 27
 Maximum EIRP                   : 27

 VAP configurations:
  WLAN ID 1:
   SSID                         : HUAWEI-WLAN
   Forward mode                 : direct-forward
   Authen mode                  : Open
   Encrypt mode                 : -
   Service vlan                 : 100
------------------------------------------------------------------------------
Radio 1 configurations:
 Radio enable                   : yes
 Work mode                      : normal
 WDS  mode                      : -
 Mesh mode                      : -
 Radio band                     : 5G
 Radio type                     : an
 Config channel/bandwidth       : -/20M
 Actual channel/bandwidth       : 157/20M
 Config EIRP                    : 127
 Actual EIRP                    : 28
 Maximum EIRP                   : 28

 VAP configurations:
  WLAN ID 1:
   SSID                         : HUAWEI-WLAN
   Forward mode                 : direct-forward
   Authen mode                  : Open
   Encrypt mode                 : -
   Service vlan                 : pool a
------------------------------------------------------------------------------
------------------------------------------------------------------------------
AP system profile          : default
Regulatory domain profile  : default
WIDS profile               : default
BLE profile                :
UUID                       :
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 XGE0            : default
 Interface XGE1            : default
 Interface XGE2            : default
 Interface XGE3            : default
 Interface Eth-trunk0      : default
Radio 0
 Radio 2.4G profile        : default
 Radio 5G profile          :
 VAP profile
  WLAN  1                  : default(VLAN 100)
 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
 Radio frequency           : 2.4G
 Spectrum analysis         : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
Radio 1
 Radio 2.4G profile        :
 Radio 5G profile          : default
 VAP profile
  WLAN  1                  : default(VLAN pool a)
 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
 Radio frequency           : 5G
 Spectrum analysis         : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
Card 1:
 Serial profile            : preset-enjoyor-toeap
 Wired port profile        :
 Iot profile               :
 UDP Port                  : -
 TCP Port                  : -
Card 2
 Serial profile            : preset-enjoyor-toeap
 Wired port profile        :
 Iot profile               :
 UDP Port                  : -
 TCP Port                  : -
Card 3
 Serial profile            : preset-enjoyor-toeap
 Wired port profile        :
 Iot profile               :
 UDP Port                  :
 TCP Port                  : -
Card usb
 Serial profile            :
 Iot profile               :
 UDP Port                  : -
 TCP Port                  : -
--------------------------------------------------------------------------------
```

Table 11-9 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 the parameter, run the **11.1.44 ap-name (AP view)** or **11.1.47 ap-rename** command.
AP group	AP group. To configure the parameter, run the **11.1.38 ap-group (AP view)** or **11.1.46 ap-regroup** command.
Country code	Country code. To configure the parameter, run the **11.1.77 country-code** command.
Radio 0 configurations/Radio 1 configurations	Radio configuration.
Radio enable	Radio status. To configure the parameter, run the **11.1.218 radio disable** command.
Work mode	Working mode of a radio. To configure the parameter, run the **11.7.88 work-mode** command.
WDS mode	WDS mode. To configure the parameter, run the **11.8.19 wds-mode** command.
Mesh mode	Mesh role of a radio. To configure the parameter, run the **11.9.21 mesh-role** command.
Radio band	Frequency band of a radio. To configure the parameter, run the **11.1.169 frequency** command.
Radio type	Protocol type of a radio.
Config channel/bandwidth	Configured AP channel and bandwidth. To configure the parameter, run the **11.1.68 channel** command.
Actual channel/bandwidth	Actual AP channel and bandwidth.

Item	Description
Config EIRP	Transmit power of a radio configured in the radio profile. To configure the parameter, run the **11.1.165 eirp** command.
Actual EIRP	Actual transmit power of a radio.
Maximum EIRP	Maximum transmit power of a radio.
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 the parameter, run the **11.1.283 vap-profile** command.
SSID	SSID name. To configure the parameter, run the **11.1.253 ssid** command.
Forward mode	Forwarding mode. To configure the parameter, run the **11.1.167 forward-mode** command.
Authen mode	Authentication mode.
Encrypt mode	Encryption mode.
Service vlan	Effective service VLAN.
AP system profile	Name of the referenced AP system profile. To configure the parameter, run the **11.1.50 ap-system-profile (AP group view and AP view)** command.
Regulatory domain profile	Name of the referenced regulatory domain profile. To configure the parameter, run the **11.1.227 regulatory-domain-profile** command.
WIDS profile	Name of the referenced WIDS profile. To configure the parameter, run the **11.7.85 wids-profile (AP group view and AP view)** command.
BLE profile	Name of the referenced BLE profile.

Item	Description
UUID	UUID of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure the parameter, run the **11.6.14 broadcasting-content (AP group view and AP view)** command.
AP wired port profile	Name of the referenced AP wired port profile. To configure the parameter, run the **11.1.292 wired-port-profile (AP group view and view)** command.
Interface *interface-name*	Interface name and number.
Radio 0/Radio 1	Radio frequency.
Radio 2.4G profile	Name of the referenced 2G radio profile. To configure the parameter, run the **11.1.220 radio-2g-profile** command.
Radio 5G profile	Name of the referenced 5G radio profile. To configure the parameter, run the **11.1.222 radio-5g-profile** command.
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 the parameter, run the **11.1.283 vap-profile** command.
Mesh profile	Name of the referenced Mesh profile. To configure the parameter, run the **11.9.19 mesh-profile radio** command.
WDS profile	Name of the referenced WDS profile. To configure the parameter, run the **11.8.22 wds-profile radio** command.
Mesh whitelist profile	Mesh whitelist profile referenced by an AP group. To configure the parameter, run the **11.9.23 mesh-whitelist-profile (AP group radio view or AP radio view)** command.

Item	Description
WDS whitelist profile	WDS whitelist profile referenced by an AP group. To configure the parameter, run the **11.8.25 wds-whitelist-profile (AP group radio view or AP radio view)** command.
Location profile	Name of the referenced location profile. To configure the parameter, run the **11.6.28 location-profile** command.
Radio switch	Radio status. To configure the parameter, run the **11.1.218 radio disable** command.
Channel	Working channel of a radio. To configure the parameter, run the **11.1.68 channel** command.
Channel bandwidth	Working bandwidth of a radio. To configure the parameter, run the **11.1.68 channel** command.
EIRP(dBm)	Transmit power of a radio, in dBm. To configure the parameter, run the **11.1.165 eirp** command.
Antenna gain(dB)	Antenna gain of a radio, in dB. To configure the parameter, run the **11.1.14 antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter, in 100 m. To configure the parameter, run the **11.1.78 coverage distance** command.
Work mode	Working mode of an AP. To configure the parameter, run the **11.7.88 work-mode** command.
Radio frequency	Working frequency band of a radio. To configure the parameter, run the **11.1.169 frequency** command.
Spectrum analysis	Whether spectrum analysis is enabled. To configure the parameter, run the **11.3.5 spectrum-analysis enable** command.

Item	Description
WIDS device detect	Whether wireless device detection is enabled. To configure the parameter, run the **11.7.81 wids device detect enable** command.
WIDS attack detect	Whether attack detection is enabled. To configure the parameter, run the **11.7.79 wids attack detect enable** command.
WIDS contain switch	Whether rogue device containment is enabled. To configure the parameter, run the **11.7.80 wids contain enable** command.
Card 1/Card 2/Card 3/Card usb	IoT card.
Serial profile	Bound serial profile. To configure the parameter, run the **11.11.20 serial-profile (IoT card interface view)** command.
Iot profile	Bound IoT profile. To configure the parameter, run the **11.11.16 iot-profile (IoT card interface view)** command.
UDP Port	UDP port.
Wired port profile	Bound AP wired port profile. To configure the parameter, run the **11.11.25 wired-port-profile (IoT card interface view)** command.
TCP Port	TCP port.

11.1.92 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-id** *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-id *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

Different countries or regions use different wireless channels and powers. Setting country and area codes can specify channels that can be used on WLANs of different countries. The **display ap configurable channel** command displays the configurable channels supported by a specified AP.

Example

# Display configurable channels supported by AP **huawei**.

```
<HUAWEI> display ap configurable channel ap-name huawei
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.
```

Table 11-10 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.
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.

11.1.93 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.	-

Parameter	Description	Value
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    00d5-ada8-1c00   default    30.1111111°E        40.2222222°N
1    244c-075f-ec20   default    110°59′59"W         77°25′53″N
2    644c-075f-ec20   default    -                   -
---------------------------------------------------------------------------------------------------------
Total: 3
```

Table 11-11 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

Item	Description
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

Related Topics

11.1.75 coordinate

11.1.94 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 AP **huawei**.

```
<HUAWEI> display ap elabel ap-name huawei
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=AP6310SN-GN-CN
BarCode=210235449210CB000011
Item=02354492
Description=AP6310SN-GN Bundle(11n,Distributed AP Indoor,Single Frequency,AC/DC
adapter(CN))
Manufactured=2012-11-27
VendorName=Huawei
IssueNumber=00
CLEICode=
BOM=
```

Table 11-12 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    dcd2-fc04-b500 L1_001    AP7110DN-AGN 210235555310CC000094 -
2    dcd2-fc9d-0bb0 1         AP7110SN-GN  210235568010D1000032 -
-------------------------------------------------------------------------------
Total: 2
```

Table 11-13 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.

11.1.95 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 11-14 Description of the **display ap global configuration** command output

Item	Description
AP auth-mode	AP authentication mode. To configure the parameter, run the **11.1.15 ap auth-mode** command.
AP LLDP switch	Whether LLDP is enabled on an AP. To configure the parameter, run the **11.1.19 ap lldp enable** command.
AP username/password	User name and password for AP login. To configure the parameter, run the **11.1.33 ap username** command.
AP data collection	Whether data buffering is enabled on an AP. To configure the parameter, run the **11.1.17 ap data-collection enable** command.
AP data collection interval(minute)	AP data buffering duration. To configure the parameter, run the **11.1.18 ap data-collection interval** command.

Related Topics

11.1.15 ap auth-mode

11.1.19 ap lldp enable

11.1.33 ap username

11.1.17 ap data-collection enable

11.1.18 ap data-collection interval

11.1.96 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 of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays LLDP neighbor information of the AP with a specified ID.	The AP ID must exist.
interface *interface-type interface-number*	Displays LLDP neighbor information on a specified AP interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
brief	Displays brief LLDP neighbor information of APs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

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.

Example

# Display LLDP neighbor information on all APs.

```
<HUAWEI> display ap lldp neighbor brief
--------------------------------------------------------------------------------
Hostname  Neighbor device  Management address  Local intf  Neighbor intf       TTL
--------------------------------------------------------------------------------
huawei    Quidway          10.10.10.3          GE0         GigabitEthernet0/0/16  119
```

```
------------------------------------------------------------------------------------
Total: 1
```

Table 11-15 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 AP **huawei**.

```
<HUAWEI> display ap lldp neighbor ap-name huawei interface gigabitethernet 0
------------------------------------------------------------------------------
AP 1 Port 0 has 1 neighbor(s):

Basic port information
------------------------------------------------------------------------------
Neighbor index              : 1
Host Name                   : huawei
Chassis ID type             : macAddress
Chassis ID                  : 5489-9876-b7d7
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 (S5720HI V200R011C00V200R011C10)
                 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
------------------------------------------------------------------------------
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 11-16 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 the 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.
Power port class	PoE type: ● PSE: power-sourcing equipment. ● PD: powered device. ● Unknown: unknown device.
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.
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.

Item	Description
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. - 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.
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.

Item	Description
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.

Related Topics

11.1.19 ap lldp enable

11.1.97 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 value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Use 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 power 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 power 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 within the calibration period. Neighbor information ages out after 1 hour and can be queried only before aging.

Example

# Display neighbor information of AP **huawei**.

```
<HUAWEI> display ap neighbor ap-name huawei
Radio: Radio ID of AP
In control AP:
------------------------------------------------------------------------------
Radio AP ID AP name         Channel  Received RSSI(dbm)  Path loss(db)
------------------------------------------------------------------------------
0     0     e468-a352-7990  1        -38                 56
------------------------------------------------------------------------------
Total: 1

Uncontrol AP:
------------------------------------------------------------------------------
Radio  BSSID          Channel  RSSI(dBm)  SSID
------------------------------------------------------------------------------
0      0020-1306-0680 1        -79        b
1      cc53-b5ee-3d00 5        -60        test
------------------------------------------------------------------------------
Total: 2
```

Table 11-17 Description of the **display ap neighbor** command output

Item	Description
In control AP	Authorized neighboring AP.
Uncontrol AP	Unauthorized neighboring AP.
Radio	Neighboring AP detected on an AP radio.
AP ID	ID of a neighboring AP.
AP name	Name of a neighboring AP.
Channel	Channel that the authorized neighboring AP uses. **NOTE** The device displays only information about neighboring APs detected on the current channel.
Received RSSI(dbm)	Strength of signals received from neighboring APs.
Path loss(db)	Path loss.
BSSID	Basic service set identifier (BSSID) of an unauthorized neighbor.
Channel	Channel that the unauthorized neighboring AP uses.
RSSI(dBm)	Power of signals received from the neighboring AP, in dBm.

Item	Description
SSID	Service set identifier (SSID) of an unauthorized neighbor.

11.1.98 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.

Example

# Display all AP offline records.

```
<HUAWEI> display ap offline-record all
------------------------------------------------------------------------------
MAC              Last offline time     Reason
------------------------------------------------------------------------------
0023-0024-0080   2015-01-31/16:21:50   The AP name is modified.
60de-4476-e360   2015-01-31/14:02:35   An AP is deleted.
```

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

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

Item	Description
MAC	AP's MAC address.
Last offline time	Last offline time of an AP.
Reason	AP offline reason. For description of offline reasons and handling suggestions, see **Table 11-19**. For troubleshooting methods, see **An AP Goes offline Unexpectedly**.

Table 11-19 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 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: License resources for the AC to manage APs are insufficient.	Apply for a new license. Huawei's Electronic Software Delivery Platform (ESDP) is accessible from the Internet and Huawei intranet. ● Internet: **http://app.huawei.com/isdp** ● Huawei intranet: **http://w3.huawei.com/sdp**
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).	No action is required. The AP will automatically attempt to recover the link.
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 **11.1.91 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.	Check the AP 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 reset manually.
The AP restarts due to a CANBUS reset.	Contact technical support personnel.
The AP restarts due to AP interference: APs are located closely, generating interference.	Contact technical support personnel.
The AP restarts due to a chip 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.
The AP is forcibly disconnected: in specific scenarios, for example, when the CAPWAP tunnel capacity is reached.	No action is required.
CAPWAP link down for DTLS smooth: DTLS requires APs to go online again during an HA or VRRP switchover.	No action is required.
The wideband status change.	The AP goes offline due to normal configuration changes, and no action is required.

Reason Why an AP Goes Offline	Suggestion
An internal error (MSC error monitored by MFPI) occurs.	Contact technical support personnel.
An internal error (MSU error monitored by MFPI) occurs.	Contact technical support personnel.
An internal error (KAP error monitored by MFPI) occurs.	Contact technical support personnel.
An internal error (TX DMA stop) occurs.	Contact technical support personnel.
An internal error (other reason) occurs.	Contact technical support personnel.
Reboot for AP Channel-load-mode change.	No action is required.
Reset for the data link DTLS configuration change.	The configuration change causes the AP to automatically reboot, and no action is required.
Reset for the AC list configuration change.	The configuration change causes the AP to automatically reboot, and no action is required.
Reset for the change of the IP address obtaining mode.	The configuration change causes the AP to automatically reboot, and no action is required.
Reset for the IP address configuration change.	The configuration change causes the AP to automatically reboot, and no action is required.
Reset for a configuration delivery failure.	Check network connectivity. If no problem is found, contact technical support personnel.

Related Topics

11.1.231 reset ap offline-record

11.1.99 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.	-
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.

Example

# Display online failure records about the AP with the MAC address 1047-80b1-56a0.

```
<HUAWEI> display ap online-fail-record mac 1047-80b1-56a0
--------------------------------------------------------------------------------
MAC            Last fail time       Reason
--------------------------------------------------------------------------------
1047-80b1-56a0  2015-01-20/15:48:06  The AP is added to the AP blacklist.
--------------------------------------------------------------------------------
Total records: 1
```

Table 11-20 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 for the AP online failure. For description of AP online failure reasons and handling suggestions, see **Table 11-21**. For troubleshooting methods, see **AP Online Failure**.

Table 11-21 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. Huawei's Electronic Software Delivery Platform (ESDP) is accessible from the Internet and Huawei intranet. ● Internet: **http://app.huawei.com/isdp** ● Huawei intranet: **http://w3.huawei.com/sdp**
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.
CAPWAP tunnel negotiation fails.	Check whether the network connectivity is normal. If yes, 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**.
The CAPWAP tunnel fails to be established.	Check whether the network connectivity is normal. If yes, contact technical support personnel.

Reason Why an AP Fails to Go Online	Suggestion
The configuration fails to be delivered.	The device attempts to deliver the configuration again. If the failure persists, contact technical support personnel.
The versions of the AP and AC do not match.	Log in to http://support.huawei.com/enterprise and download the release notes. Based on the version mapping, upgrade the AP or AC to the matching version. ● Enterprise technical support website: **http://support.huawei.com/enterprise** ● Carrier technical support website: **http://support.huawei.com**
The AC does not support the AP type.	Replace the AP with that supported by the AC or replace the AC with one that supports this AP type.
The AP name conflicts.	Run the **11.1.47 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.
The central AP is not in normal state.	Run the **11.1.87 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.
The configured and reported AP types are different.	Ensure that the configured AP type is the same as the reported one.

Related Topics

11.1.232 reset ap online-fail-record

11.1.100 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

Currently, optical module information query is supported only by the AP6610DN-AGN, AP6610DN-AGN-US, AP9131DN, AP9132DN, AP8050TN-HD, AP8082DN, AP8182DN, AP8130DN-W, AP8030DN, AP8050DN, AP8050DN-S, AP8150DN, and AP8130DN.

Precautions

If an electrical module is inserted into an optical interface, diagnostic information is not supported.

Example

# Display optical module information of AP **huawei**.

```
<HUAWEI> display ap optical-info ap-name huawei
-------------------------------------------------------------------------------
Interface name:XGE0/0/0
-------------------------------------------------------------------------------
Common information:
  Transceiver Type                   :1000_BASE_LX_SFP
  Connector Type                     :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:
  Manu. 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
  Voltage(0.1mV)                     :33161
  Volt High Threshold(0.1mV)         :37000
  Volt Low Threshold(0.1mV)          :29000
  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 Type                     :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:
  Manu. 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
  Voltage(0.1mV)                     :32808
  Volt High Threshold(0.1mV)          :34461
  Volt Low Threshold(0.1mV)           :30523
  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 Type                     :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:
  Manu. 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
  Voltage(0.1mV)                     :32776
  Volt High Threshold(0.1mV)          :35650
  Volt Low Threshold(0.1mV)           :29000
  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 Type                     :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:
  Manu. 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
  Voltage(0.1mV)                      :33061
  Volt High Threshold(0.1mV)          :37000
  Volt Low Threshold(0.1mV)           :29000
  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 11-22 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 Type	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.
Manu. Serial Number	Vendor sequence number of the optical module.
Manufacturing Date	Manufacturing date of the optical module.

Item	Description
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.
Temp Low Threshold(degree C)	The lower threshold for the temperature of the optical module, in °C.
Voltage(0.1mV)	Current voltage of the optical module, in 0.1mV.
Volt High Threshold(0.1mV)	The upper threshold for the voltage of the optical module, in 0.1mV.
Volt Low Threshold(0.1mV)	The lower threshold for the voltage of the optical module, in 0.1mV.
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 0.1uw.
RX Power High Threshold(0.1uw)	Upper receive power threshold for the optical module, in 0.1uw.
RX Power Low Threshold(0.1uw)	Lower receive power threshold for the optical module, in 0.1uw.
TX Power(0.1uw)	Transmit power of the optical module, in 0.1uw.
TX Power High Threshold(0.1uw)	Upper transmit power threshold for the optical module, in 0.1uw.
TX Power Low Threshold(0.1uw)	Lower transmit power threshold for the optical module, in 0.1uw.

11.1.101 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
Temperature(degree C)          : 54
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 11-23 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.
Temperature(degree C)	AP's internal temperature (°C). **NOTE** The temperature is displayed as "-" for APs that do not support the temperature check.
Online user number	Number of online users.
Upstream traffic(wireless)(KB)	Traffic volume on the wireless upstream interface in a specified period, in KB.
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 the wired-side 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.

Item	Description
port total Bytes(TX)	Number of bytes sent by the wired-side 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).

11.1.102 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 provisioning view.

```
<HUAWEI> display ap provision ap-id 2
------------------------------------------------------------------------------
AP name                : 70d9-313c-3120
AP group               : default
AP address mode        : static
IPv4 address           : -
IPv4 mask address      : -
IPv4 gateway address   : -
IPv4 AC list           : -
------------------------------------------------------------------------------
```

Table 11-24 Description of the **display provision-ap parameter-list** command output

Item	Description
AP name	AP name. To configure this parameter, run the **11.1.44 ap-name (AP view)** command.
AP group	AP group to which an AP belongs. To configure this parameter, run the **11.1.38 ap-group (AP view)** command.
AP address mode	Mode in which an AP obtains an IP address. To configure this parameter, run the **11.1.8 address-mode (AP view)** command.
IPv4 address	Static IPv4 address of an AP. To configure this parameter, run the **11.1.175 ip-address (AP view)** command.
IPv4 mask address	Static IPv4 mask of an AP. To configure this parameter, run the **11.1.175 ip-address (AP view)** command.
IPv4 gateway address	IPv4 gateway address of an AP. To configure this parameter, run the **11.1.175 ip-address (AP view)** command.
IPv4 AC list	AC IPv4 address list for APs. To configure this parameter, run the **11.1.5 ac-list (AP view)** command.

Related Topics

11.1.5 ac-list (AP view)

11.1.8 address-mode (AP view)
11.1.38 ap-group (AP view)
11.1.44 ap-name (AP view)
11.1.175 ip-address (AP view)

11.1.103 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.
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 port status and traffic information of online APs, which facilitates AP port maintenance and management.

Example

# Display port status and traffic information of all APs.

```
<HUAWEI> display ap port all
Info: Waiting for AP response.
```

```
-------------------------------------------------------------------------------------------------------------------------------
-----
AP-ID Port      State Speed Duplex TX-Packets      Tx-ErrorPackets  TX-Rate(Kbps) RX-Packets      RX-
DropPackets   RX-Rate(Kbps)
-------------------------------------------------------------------------------------------------------------------------------
-----
0     GE0      up    1000  full   9178          0            0          12857          0             1
-------------------------------------------------------------------------------------------------------------------------------
-----
Printed: 1
```

Table 11-25 Description of the **display ap port** command output

Parameter	Description
AP-ID	AP ID.
Port	AP port.
State	Status of the AP port. ● down: The AP port is Down. ● up: The AP port is Up. ● *down: The interface is shut down.
Speed	Speed of the AP port, in Mbit/s.
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.

11.1.104 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     dcd2-fcf6-76a0    ap_1    default   AT(FULL)           LLDP
1     60de-4474-9640    ap_2    default   AF(RESTRICTED)     AP capability
------------------------------------------------------------------------------------------------------------------------------------
-----
Total: 2
```

Table 11-26 Description of the **display ap power-workmode** command output

Item	Description
ID	AP ID.
MAC	AP MAC address.
Name	AP name.
Group	AP group to which an AP belongs.
Power-workmode	Current power mode of an AP. ● The power mode of an AP can be AF, AT, or BT, which represents 802.3af, 802.3at, or 802.3bt, respectively. ● The working mode of an AP can be FULL or RESTRICTED, which indicates that functions of the AP are unrestricted and partially restricted, respectively.
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

11.1.105 display ap resource

Function

The **display ap resource** command displays the number of CAPWAP tunnel resources used by APs on a switch.

Format

display ap resource slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a switch.	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 switch.

Example

# Display the number of CAPWAP tunnel resources used by APs on a switch.

```
<HUAWEI> display ap resource slot 0
Slot  0
---------------------------------------------------------------------------
Number Used :0
Number Free : 1024
Number Total: 1024
```

Table 11-27 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	Number of CAPWAP tunnel resources on a switch.

11.1.106 display ap run-info

Function

The **display ap run-info** command displays 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 running status of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays 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 AP running status. You can run this command to monitor an AP in real time.

Prerequisites

The AP works properly.

Example

# Display running status of AP **huawei**.

```
<HUAWEI> display ap run-info ap-name huawei
------------------------------------------------------------------------------
AP type                        : AP7030DE
Country code                   : CN
Software version               : V200R007C10
Hardware version               : Ver.A
BIOS version                   : 271
BOM version                    : 001
Memory size(MB)                : 256
Flash size(MB)                 : 64
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
IP address                     : 192.168.109.252
IP mask                        : 255.255.255.0
Gateway                        : 192.168.109.1
DNS server                     : 0.0.0.0
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 1: -, slot 2: -, slot 3: -
------------------------------------------------------------------------------
```

Table 11-28 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.
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.
IP address	AP IPv4 address.
IP mask	Mask of an AP.
Gateway	Gateway IP address of an AP.
DNS server	IP address of the DNS server.
XGigabitEthernet port number	ID of the AP's XGigabitEthernet port. Only AD9431DN-24X series APs have XGigabitEthernet ports.
MultiGE port number	ID of the AP's MultiGE port. Only AP7050DN-E, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8082DN, and AP8182DN series APs have MultiGE ports.
GigabitEthernet port number	ID of the AP's Ethernet interface.
Port speed(Mbps)	Rate on the upstream Ethernet interface, in Mbit/s.

Item	Description
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.
Port state	AP interface status. ● down: indicates that the interface is disabled. ● up: indicates that the interface is enabled. ● *down: indicates that the interface is shut down.
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.

11.1.107 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.

Parameter	Description	Value
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 value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

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 **huawei**.

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

Table 11-29 Description of the **display ap sta-signal strength** command output

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

11.1.108 display ap statistics

Function

The **display ap statistics** command displays statistics on the types of APs added to an AC.

Format

display ap statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

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

Example

# Display statistics about AP types.

```
<HUAWEI> display ap statistics
--------------------------------------------------------------------------------
Type              Number
--------------------------------------------------------------------------------
AP6010DN-AGN        1
AP6510DN-AGN        1
AP5010DN-AGN        1
--------------------------------------------------------------------------------
```

Table 11-30 Description of the **display ap statistics** command output

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

11.1.109 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.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
radio *radio-id*	Specifies the radio ID.	The value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.
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.

Example

# Display statistics about packets with the SSID **cmcc** on radio 0 of an AP **huawei**.

```
<HUAWEI> display ap traffic statistics wireless ap-name huawei 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 11-31 Description of the **display ap traffic statistics wireless ap-name** *ap-name* **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.
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 **huawei**.

```
<HUAWEI> display ap traffic statistics wireless ap-name huawei 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 maximal signal strength(dBm)(RX)        :0
Wireless minimal signal strength(dBm)(RX)        :0
Wireless average signal strength(dBm)(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 drop rate(%)                        :0
Wireless port drop rate 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 PER(%)                                  :0
WMM AC_BK PER(%)                                  :0
WMM AC_VI PER(%)                                  :0
WMM AC_VO PER(%)                                  :0
------------------------------------------------------------------------
```

Table 11-32 Description of the **display ap traffic statistics wireless ap-name** *ap-name* **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)	Number of unicast frames received by the radio.
Wireless management frames(RX)	Number of management frames received by the radio.

Item	Description
Wireless data frames(RX)	Number of data frames received by the radio.
Wireless maximal signal strength(dBm)(RX)	Maximum strength of signals received by the radio, in dBm.
Wireless minimal signal strength(dBm)(RX)	Minimum strength of signals received by the radio, in dBm.
Wireless average signal strength(dBm)(RX)	Average strength of signals received by the radio, in dBm.
Wireless frames(TX)	Number of transmitted frames received by the radio.
Wireless bytes(TX)	Total number of bytes of data frames transmitted by the radio.
Wireless RTS successes(TX)	Number of Request to Send (RTS) frames that are successfully sent by the radio.
Wireless unicast frames(TX)	Number of transmitted unicast frames received by the radio.
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 (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.

Item	Description
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 last statistical period.
Wireless port drop rate(%)	Packet loss ratio of the radio.
Wireless port drop rate of the last 5min(%)	Packet loss ratio of the radio in the last statistical period.
Wireless retransmitted rate(%)	Retransmission ratio of the radio.
Wireless retransmitted rate of the last 5min(%)	Retransmission ratio of the radio in the last statistical period.
Wireless channel utilization(%)	Channel usage 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 ratio 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 PER(%)	PER of AC_BE packets in the WMM queue.
WMM AC_BK PER(%)	PER of AC_BK packets in the WMM queue.
WMM AC_VI PER(%)	PER of AC_VI packets in the WMM queue.
WMM AC_VO PER(%)	PER of AC_VO packets in the WMM queue.

11.1.110 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 authentication or SN authentication mode is configured for an AP but the AP is neither added offline 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 unauthenticated APs.

Example

# Display information about unauthenticated APs.

```
<HUAWEI> display ap unauthorized record
Unauthorized AP record:
Total number: 1
--------------------------------------------------------------------------------
AP type: AP7110SN-GN
AP SN: 210235568010D1000032
AP MAC address: dcd2-fc9d-0bb0
AP IP address: 192.168.109.252
Record time: 2015-01-22 17:23:17
--------------------------------------------------------------------------------
```

Table 11-33 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	Type of an unauthenticated AP.

Item	Description
AP SN	Serial number of an unauthenticated AP.
AP MAC address	MAC address of an unauthenticated AP.
AP IP address	IP address of an unauthenticated AP.
Record time	Time when an unauthorized AP is recorded.

11.1.111 display ap uncontrol all

Function

The **display ap uncontrol all** command displays information about all APs that are not controlled 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 APs that are not controlled by the local AC.

```
<HUAWEI> display ap uncontrol all
--------------------------------------------------------
BSSID          NEAREST-AP      CHANNEL  RSSI(dBm)   SSID
--------------------------------------------------------
1047-80af-9970 ap-13           149      -68         test
```

```
----------------------------------------------------------
Total: 1
```

Table 11-34 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.

11.1.112 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 the display ap update configuration command to view AP upgrade configuration, including the upgrade mode, FTP server configuration, and SFTP server configuration.

Example

# Display AP upgrade configuration.

```
<HUAWEI> display ap update configuration
--------------------------------------------------------------------------------
AP update mode          : AC-mode
FTP configuration
 FTP IP                 : -
 FTP username           : anonymous
 FTP password           : ******
 FTP max number         : 50
SFTP configuration
 SFTP IP                : -
 SFTP username          : anonymous
 SFTP password          : ******
 SFTP 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
 AP6010DN-AGN           : FitAP6X10XN_V200R007C20.bin
--------------------------------------------------------------------------------
```

Table 11-35 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 the parameter, run the **11.1.25 ap update mode** command.
FTP configuration	FTP server configuration.
FTP IP	IP address of the FTP server. To configure the parameter, run the **11.1.22 ap update ftp-server** command.
FTP username	User name for logging in to the FTP server. To configure the parameter, run the **11.1.22 ap update ftp-server** command.
FTP password	Password for logging in to the FTP server. To configure the parameter, run the **11.1.22 ap update ftp-server** command.

Item	Description
FTP max number	Maximum number of APs that can be upgraded simultaneously in FTP mode. To configure the parameter, run the **11.1.22 ap update ftp-server** command.
SFTP configuration	SFTP server configuration.
SFTP IP	IP address of the SFTP server. To configure the parameter, run the **11.1.29 ap update sftp-server** command.
SFTP username	User name for logging in to the SFTP server. To configure the parameter, run the **11.1.29 ap update sftp-server** command.
SFTP password	Password for logging in to the SFTP server. To configure the parameter, run the **11.1.29 ap update sftp-server** command.
SFTP max number	Maximum number of APs that can be upgraded simultaneously in SFTP mode. To configure the parameter, run the **11.1.29 ap update sftp-server** command.
AP update schedule-task	ID of a scheduled AP upgrade task. To configure the parameter, run the **11.1.32 ap update schedule-task** command.
AP type/AP-group update filename	Name of the upgrade file for a specified AP type or group. To configure the parameter, run the **11.1.31 ap update update-filename** command.

11.1.113 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

# View information about scheduled AP upgrade task.

```
<HUAWEI> display ap update schedule-task
--------------------------------------------------------------------------------
 Task-ID  Task-State  Start-Time        Stop-Time         AP-Type  AP-Group
--------------------------------------------------------------------------------
 1        IDLE        2016/11/01 11:11  2017/01/01 11:12  54       -
--------------------------------------------------------------------------------
```

Table 11-36 Description of the **display ap update schedule-task** command output

Item	Description
Task-ID	ID of a scheduled AP upgrade task.

Item	Description
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.

Related Topics

11.1.32 ap update schedule-task

11.1.114 display ap update status

Function

The **display ap update status** command displays AP upgrade progress.

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* }

Parameters

Parameter	Description	Value
all	Displays upgrade progress of all APs.	-
downloading	Displays APs that are upgrading.	-

Parameter	Description	Value
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 AP name must exist.
ap-id *ap-id*	Displays upgrade progress of the AP with a specified ID.	The AP ID must exist.
ap-type *ap-type*	Displays upgrade progress of APs of a specified type.	The value is an integer. To view all RU 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.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check upgrade progress of all APs or a specified AP, and check information about APs in specified upgrade status.

Example

# Display upgrade progress of all APs.

```
<HUAWEI> display ap update status all
FT : File Type
------------------------------------------------------------------------------------------------------------------------
----------------
ID   Name   AP Type       AP Group   AP MAC          FT     Update Version     Last Update Time   Update
Status
------------------------------------------------------------------------------------------------------------------------
----------------
0    hw0    AP6010DN-AGN  default    60de-4476-e320  FIT    V200R008C10B008    2016/08/22 18:51
succeed
1    hw1    AP6010DN-AGN  default    60de-4476-e340  FIT    V200R008C10B008    2016/08/22 18:51
downloading(progress: 80%/0%)
2    hw2    AP6010DN-AGN  default    60de-4476-e360  FIT    V200R008C10B008    2016/08/22 18:51
downloading(progress: 100%/50%)
3    hw3    AP6010DN-AGN  default    60de-4476-e380  FIT    -                  -                  -
```

```
4    hw4    AP6010DN-AGN  default    60de-4476-e3a0  FIT    -              -               -
5    hw5    AP6010DN-AGN  default    60de-4476-e3c0  FIT    -              -               -
--------------------------------------------------------------------------------------------------------------------------------------
----------------
Total: 6
```

Table 11-37 Description of the **display ap update status all** command

Item	Description
ID	AP ID.
Name	AP name.
AP Type	AP type.
AP Group	AP group.
AP MAC	MAC address of the AP.
FT	Type of the AP upgrade file.
Update Version	Target version that an AP is upgraded to.
Last Update Time	Last end time when an AP is upgraded.

Item	Description
Update Status	AP upgrade progress. ● downloading (progress: 80%/0%): The AP is downloading the system software package, with 80% downloaded. ● downloading (progress: 100%/50%): The system software package is successfully downloaded and is being written to the flash memory, with 50% written. ● 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. In this situation, the actual RU upgrade result depends on that displayed in the **display ap update status all** command output. ● failed(alloc memory for file): The upgrade failed because the AP failed to apply for memory resources. ● failed(AP is updating now. Please wait.): The upgrade failed. Before VRRP switchover, the AP upgrades online in AC mode. After VRRP switchover, the AP upgrade is not complete and the AC delivers the upgrade command again. Therefore, the system prompts that the upgrade fails. ● 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. ● failed(AP type mismatch batch upgrade AP type): The upgrade failed because the AP type is different from the batch upgrade AP type.

Item	Description
	● failed(AP wait file timeout): The upgrade failed because the time that the AP waits for fragment data expired. ● failed(block full): The upgrade failed because the number of APs simultaneously upgraded in AC mode reaches the maximum. ● failed(change to standby): The upgrade failed due a revertive switchover failure. ● failed(fail to download the file): The upgrade failed because the system software failed to be downloaded. ● failed(file content error): The upgrade failed due to incorrect system software file contents. ● 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. ● failed(invalid file name): The upgrade failed because the name of the AP version file is incorrect. ● failed(link down): The upgrade failed because the AP failed to communicate with the AC. ● failed(mode changed): The upgrade failed because the AP upgrade mode is changed during the AP automatic upgrade. ● failed(nospace in AP memory): The upgrade failed because the AP memory resources were insufficient. ● failed(not receive update result): The upgrade failed because the AC receives no AP upgrade result. ● failed(over max upgrade time): The upgrade failed because the upgrade duration exceeds the maximum upgrade time allowed. ● failed(server password is too long): The upgrade failed because the FTP/SFTP server password is too long.

Item	Description
	● failed(read file): The upgrade failed because no upgrade file is available in the flash memory. ● failed(receive file failed): The upgrade failed because fragments failed to be received. ● failed(retransfer over times): The upgrade failed because the number of fragment retransmissions exceeds the threshold. ● failed(send first file failed): The upgrade failed because the first fragment failed to be sent. ● failed(other reason): The upgrade failed due to an unknown error. ● failed(upgrade timeout): The upgrade timed out and failed. ● failed(user canceled): The upgrade failed because the user canceled the upgrade. ● failed(waited for next batch): The upgrade failed. The AP has to wait for the next upgrade. ● failed(write flash error): The upgrade failed because the system software package failed to be written to the flash memory. ● failed(file changed): The upgrade failed because the upgrade file was modified during the automatic upgrade. ● failed(age time out): The upgrade failed because the state machine aged out. ● succeed: The upgrade succeeded. ● succeed(auto resetting): The upgrade failed, and the AP is being restarted. ● succeed(need reset): The upgrade succeeded. The AP must be restarted. ● succeed(resetting): The upgrade succeeded and the AP is being manually restarted.

Item	Description
	● succeed(no need to update): The upgrade succeeded. There is no need to upgrade the AP. ● succeed(need mode switch): The upgrade succeeded. The AP mode needs to be switched. ● failed(send upgrade configuration): The upgrade failed because the upgrade configuration failed to be sent. ● failed(send upgrade request): The upgrade failed because the upgrade request failed to be sent. ● failed(upgrade configuration response error): The upgrade failed because there was an error in the AP's upgrade response. ● failed(process upgrade filename): The upgrade failed because the AC failed to process the upgrade file name. ● failed(cannot get AP type): The upgrade failed because the AC failed to obtain the AP type. ● failed(analyze the version by upgrade filename): The upgrade failed because the device failed to analyze the version number in the file name. ● failed(age time out): The upgrade failed because the state machine aged out. ● 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. ● -: The AP requires no upgrade. ● failed(flash component change): The upgrade failed because the flash model is not supported. ● failed (Backing up the system software): The upgrade failed because the system software is being synchronized from the main area to the standby area.

Item	Description
	- -: The AP requires no upgrade.

Related Topics

11.1.24 ap update load

11.1.26 ap update multi-load

11.1.115 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

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 11-38 Description of the **display ap username** command output

Item	Description
AP username	User name for logging in to the AP. To configure the parameter, run the **11.1.33 ap username** command.
AP password	Password for logging in to the AP. To configure the parameter, run the **11.1.33 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.
Password alert original	Whether to enable the initial password change prompt function.
Password expired	Whether a password expires.

Related Topics

11.1.33 ap username

11.1.116 display ap version

Function

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

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.	-

Parameter	Description	Value
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 **VxxxRxxxCxxxSPCxx**. For example, V200R006C00 or V200R005C10SPC200.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap version** command to view AP version information.

Example

# Display version information about all APs.

```
<HUAWEI> display ap version all
Compatible version : V200R008 V200R007 V200R006C10 V200R006C20
-------------------------------------------------------------------------------
ID    Name           Group   Type           Version           state
-------------------------------------------------------------------------------
0    60de-4476-e360 default AP6010DN-AGN    V200R007C20        normal
-------------------------------------------------------------------------------
Total: 1
```

Table 11-39 Description of the **display ap version** command output

Item	Description
Compatible version	Compatible version.
ID	Index
Name	AP name.
Group	AP group name.

Item	Description
Type	AP type.
Version	AP version name.
state	AP state. For details, see **Table 11-5**.

Table 11-40 AP state list

AP State	Description	Possible Cause	Handling Suggestion
commit-failed	WLAN service configurations fail to be delivered to an AP after the AP goes online on an AC.	After the 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	WLAN service configurations are being delivered to an AP after the AP goes online on an AC.	After the AP goes online on the AC, WLAN service configurations are being delivered to the AP.	This is a normal state, and no action is required.
config	WLAN service configurations are being delivered to an AP when the AP is going online on an AC.	After the 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	WLAN service configurations fail to be delivered to an AP when the AP is going online on an AC.	After the 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	An AP is in upgrade state.	When the 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.	The 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.	Handle the AP online failure. For details, see **AP Online Failure** in the *Troubleshooting Insights*.

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.	The AP has not established a CAPWAP link with the AC, the MAC address and SN of the AP that is added offline are different from the actual ones, or license resources are insufficient.	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 obtain 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**

AP State	Description	Possible Cause	Handling Suggestion
			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 license resources of the AC.
name-conflicted	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	An AP is working properly.	An AP successfully goes online on an AC.	This is a normal state, and no action is required.
standby	The AP is in normal state on the standby AC.	In the HSB, dual-link cold backup, or N+1 backup scenario, if the link between the active and standby ACs is established properly, the AP is in standby state on the standby AC and in normal state on the active AC.	This is a normal state, and no action is required.

AP State	Description	Possible Cause	Handling Suggestion
ver-mismatch	The version of an AP does not match that of an AC on which the AP is to go online.	The versions of the AP and the AC mismatch.	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: **http://support.huawei.com/enterprise** ● Carrier technical support website: **http://support.huawei.com**
countryCode-mismatch	The country code of an AP does not match that of the AC on which the AP is about to go online.	The current version of the AP does not support the country code configured on the AC.	The AP does not support the country code. Upgrade the AP or change the country code configured on the AC.
unauthed	The AP is not authenticated.	The AP fails to be authenticated.	Run the **ap-confirm** command to confirm unauthenticated APs and allow them to go online.

11.1.117 display ap whitelist

Function

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

Format

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

Parameters

Parameter	Description	Value
sn	Displays serial numbers (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 authentication or SN authentication using the **11.1.15 ap auth-mode** command, you can run the **11.1.34 ap whitelist** command to configure an AP whitelist. Only APs on the whitelist are allowed to go online. To check information about APs 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      1047-80b1-56a0
1      0023-0024-0080
2      dcd2-fc9d-0bb0
--------------------------------------------------------------------------------
Total: 3
```

Table 11-41 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 11-42 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.

Related Topics

11.1.34 ap whitelist

11.1.118 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 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 the AP wired interface.

Example

# Display GE interface configuration of AP **huawei**.

```
<HUAWEI> display ap wired-port gigabitethernet 0 ap-name huawei
------------------------------------------------------------------------------
Wired port number            : 0
Wired port type              : GigabitEthernet
Wired port description       :
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           IPv6 ACL 3011
--------------------------------------------------------------------------------------------
------------------------------------------------------------------------------
```

Table 11-43 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 STP	Whether to enable STP on the wired interface.
Wired port user isolate	Whether to enable user isolation 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 to enable LLDP on the wired interface.
Wired port LLDP basic TLV management address	Management IP address of the wired interface.
Wired port LLDP basic TLV port description	Wired interface description.
Wired port LLDP basic TLV system capability	Wired interface capability set.
Wired port LLDP basic TLV system description	Wired interface system description.
Wired port LLDP basic TLV system name	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.
Wired port CRC warn low threshold	Lower alarm threshold for CRC errors on the wired interface.

Item	Description
Wired port IPv4 inbound ACL number	IPv4-based ACL in the inbound direction.
Wired port IPv4 outbound ACL number	IPv4-based ACL in the outbound direction.
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 Eth-trunk interface configuration of AP **huawei**.

```
<HUAWEI> display ap wired-port eth-trunk 0 ap-name huawei
----------------------------------------------------------------------------
Eth-trunk ID                    : 0
Eth-trunk description           : -
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            IPv6 ACL 3011
----------------------------------------------------------------------------------------
----------------------------------------------------------------------------
```

Table 11-44 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.

Item	Description
Eth-trunk description	Description of the Eth-trunk interface.
STP	Whether to enable STP on the Eth-trunk interface.
User isolate	Whether to enable user isolation 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

11.1.119 display ap-group

Function

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

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 an AP group.

Example

# Display information about all AP groups.

```
<HUAWEI> display ap-group all
------------------------------------------------------------
Name                         APs
------------------------------------------------------------
default                      1
ap-group1                    0
------------------------------------------------------------
Total: 2
```

Table 11-45 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                :
UUID                       :
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 XGE0            : default
 Interface XGE1            : default
 Interface XGE2            : default
 Interface XGE3            : default
 Interface Eth-trunk0      : default
Radio 0
 Radio 2.4G profile        : default
 Radio 5G profile          : default
 VAP profile
  WLAN 15                  : default(VLAN 15)
 Mesh profile              :
 WDS profile               : default
 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
 Radio frequency           : 2.4G
 Spectrum analysis         : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
 Beacon switch             : enable
 CTS switch                : enable
 CTS delay time(us)        : none
Radio 1
 Radio 5G profile          : default
 VAP profile
  WLAN 15                  : default(VLAN pool a)
 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
 Radio frequency           : 5G
 Spectrum analysis         : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
 Beacon switch             : enable
 CTS switch                : enable
 CTS delay time(us)        : none
Radio 2
 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
 Radio frequency           : 5G
 Spectrum analysis         : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
Card 1
 Serial profile            : preset-enjoyor-toeap
 Iot profile               :
 UDP Port                  : -
Card 2
 Serial profile            : preset-enjoyor-toeap
 Iot profile               :
 UDP Port                  : -
Card 3
 Serial profile            : preset-enjoyor-toeap
 Iot profile               :
 UDP Port                  : -
```

Table 11-46 Description of the **display ap-group name** command output

Item	Description
AP system profile	AP system profile referenced by an AP group. To configure the parameter, run the **11.1.50 ap-system-profile (AP group view and AP view)** command.
Regulatory domain profile	Regulatory domain profile referenced by an AP group. To configure the parameter, run the **11.1.227 regulatory-domain-profile** command.

Item	Description
WIDS profile	WIDS profile referenced by an AP group. To configure the parameter, run the **11.7.85 wids-profile (AP group view and AP view)** command.
BLE profile	BLE profile referenced by an AP group. To configure the parameter, run the **11.6.10 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 the parameter, run the **11.6.14 broadcasting-content (AP group view and AP view)** command.
AP wired port profile	AP wired port profile referenced by an AP group. To configure the parameter, run the **11.1.292 wired-port-profile (AP group view and 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 the parameter, run the **11.1.220 radio-2g-profile** command.
Radio 5G profile	5G radio profile referenced by an AP group. To configure the parameter, run the **11.1.222 radio-5g-profile** command.
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 the parameter, run the **11.1.283 vap-profile** command.
Mesh profile	Mesh profile referenced by an AP group. To configure the parameter, run the **11.9.19 mesh-profile radio** command.

Item	Description
WDS profile	WDS profile referenced by an AP group. To configure the parameter, run the **11.8.22 wds-profile radio** command.
Mesh whitelist profile	Mesh whitelist profile referenced by an AP group. To configure the parameter, run the **11.9.23 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 the parameter, run the **11.8.25 wds-whitelist-profile (AP group radio view or AP radio view)** command.
Location profile	Location profile referenced by an AP group. To configure the parameter, run the **11.6.28 location-profile** command.
Radio switch	Whether a radio is enabled. To configure the parameter, run the **11.1.218 radio disable** command.
Channel	Working channel of a radio. To configure the parameter, run the **11.1.68 channel** command.
Channel bandwidth	Operating bandwidth of a radio. To configure the parameter, run the **11.1.68 channel** command.
EIRP(dBm)	Transmit power of a radio, in dBm. To configure the parameter, run the **11.1.165 eirp** command.
Antenna gain(dB)	Antenna gain of a radio, in dBm. To configure the parameter, run the **11.1.14 antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter (unit: 100 m). To configure the parameter, run the **11.1.78 coverage distance** command.
Work mode	Working mode of a radio. To configure the parameter, run the **11.7.88 work-mode** command.

Item	Description
Radio frequency	Working frequency of a radio. To configure the parameter, run the **11.1.169 frequency** command.
Spectrum analysis	Whether spectrum analysis is enabled. To configure the parameter, run the **11.3.5 spectrum-analysis enable** command.
WIDS device detect	Whether wireless device detection is enabled. To configure the parameter, run the **11.7.81 wids device detect enable** command.
WIDS attack detect	Whether attack detection is enabled. To configure the parameter, run the **11.7.79 wids attack detect enable** command.
WIDS contain switch	Whether rogue device containment is enabled. To configure the parameter, run the **11.7.80 wids contain enable** command.
Beacon switch	Whether RUs are enabled to send Beacon frames. To configure this parameter, run the **11.4.2 beacon disable** command.
CTS switch	Whether RUs are enabled to respond to STAs with CTS packets. To configure this parameter, run the **11.4.4 cts disable** command.
CTS delay time(us)	Delay time after which RUs respond to STAs with CTS packets. To configure this parameter, run the **11.4.3 cts delay** command.
Card 1/Card 2/Card 3/Card usb	IoT card.
Serial profile	Bound serial profile. To configure the parameter, run the **11.11.20 serial-profile (IoT card interface view)** command.
Iot profile	Bound IoT profile. To configure the parameter, run the **11.11.16 iot-profile (IoT card interface view)** command.

Item	Description
UDP Port	UDP port.
Wired port profile	Bound AP wired port profile. To configure the parameter, run the **11.11.25 wired-port-profile (IoT card interface view)** command.
TCP Port	TCP port.

Related Topics

11.1.36 ap-group

11.1.120 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 the **display ap-system-profile** 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 11-47 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 **default**.

```
<HUAWEI> display ap-system-profile name default
----------------------------------------------------------------------------------
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
Card connect type                                  : serial
Mesh role                                          : mesh-node
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 high temperature threshold(degree C)            : -
AP low temperature threshold(degree C)             : -
AP CPU usage threshold(%)                          : 90
AP memory usage threshold(%)                       : 80
Alarm restriction                                  : enable
Alarm restriction period(s)                        : 60
Log server IP address                              : -
Log record level                                   : info
Ethernet port MTU(byte)                            : 1500
Telnet                                             : disable
STelnet server                                     : enable
SFTP server                                        : enable
Console                                            : enable
```

```
Antenna output mode                          : split
Led                                    : on
Led off time range                          : -
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
  User interface vty 1
    Idle timeout                          : 5min 0s
    Screen length                          : 24
  User interface vty 2
    Idle timeout                          : 5min 0s
    Screen length                          : 24
  User interface vty 3
    Idle timeout                          : 5min 0s
    Screen length                          : 24
  User interface vty 4
    Idle timeout                          : 5min 0s
    Screen length                          : 24
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
------------------------------------------------------------------------------
```

Table 11-48 Description of the **display ap-system-profile name** *profile-name* command output

Item	Description
AC priority	AC priority. To configure the parameter, run the **11.13.14 priority** command.
Protect AC IP address	IP address of the standby AC. To configure the parameter, run the **11.13.15 protect-ac** command.
Primary AC	IP address of the primary AC. To configure the parameter, run the **11.13.13 primary-access** command.
Backup AC	IP address of the backup AC. To configure the parameter, run the **11.13.11 backup-access** command.

Item	Description
AP management VLAN	Management VLAN of an AP. To configure the parameter, run the **11.1.195 management-vlan** command.
Keep service	Whether service endurance upon CAPWAP link disconnection between the AP and AC is enabled. ● enable: This function is enabled. ● disable: This function is disabled. To configure the parameter, run the **11.1.177 keep-service enable** command.
Keep service allow new access	Whether new STAs are allowed to go online when an AP is offline. ● enable: This function is enabled. ● disable: This function is disabled. To configure the parameter, run the **11.1.178 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 the parameter, run the **11.1.178 keep-service enable allow new-access no auth** command.
Temporary management switch	Status of the offline management and antenna alignment VAPs. ● enable: This function is enabled. ● disable: This function is disabled.
Card connect type	Communication connection type between IoT cards and APs. To configure the parameter, run the **11.11.2 card connect-type** command.
Mesh role	Mesh role. To configure the parameter, run the **11.9.21 mesh-role** command.
STA access mode	STA access mode. To configure the parameter, run the **11.7.62 sta-access-mode** command.

Item	Description
STA whitelist profile	Name of a STA whitelist profile referenced by an AP system profile. To configure the parameter, run the **11.7.62 sta-access-mode** command.
STA blacklist profile	Name of a STA blacklist profile referenced by an AP system profile. To configure the parameter, run the **11.7.62 sta-access-mode** command.
EAPOL start mode	Eapol-start packet encapsulation mode. To configure the parameter, run the **11.1.164 eapol-start dest-address transform-to** command.
EAPOL start transform	Eapol-start packet conversion mode. To configure the parameter, run the **11.1.163 eapol-start dest-address transform-condition** command.
EAPOL response mode	Eapol-response packet encapsulation mode. To configure the parameter, run the **11.1.162 eapol-response dest-address transform-to** command.
EAPOL response transform	Eapol-response packet conversion mode. To configure the parameter, run the **11.1.161 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 the parameter, run the **11.1.184 lldp message-transmission delay (AP system profile view)** command.
AP LLDP message transmission hold multiplier	Hold time multiplier of AP information on neighbors. To configure the parameter, run the **11.1.185 lldp message-transmission hold-multiplier (AP system profile view)** command.

Item	Description
AP LLDP message transmission interval time(s)	Interval at which an AP sends LLDP packets to neighbors. To configure the parameter, run the **11.1.186 lldp message-transmission interval (AP system profile view)** command.
AP LLDP restart delay time(s)	Delay in re-enabling LLDP. To configure the parameter, run the **11.1.189 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 the parameter, run the **11.1.181 lldp admin-status** command.
AP LLDP report enable	Whether an AP is enabled to report information about its LLDP neighbors. To configure the parameter, run the **11.1.187 lldp report enable** command.
AP high temperature threshold(degree C)	High temperature alarm threshold of an AP. To configure the parameter, run the **11.1.171 high-temperature threshold** command.
AP low temperature threshold(degree C)	Low temperature alarm threshold of an AP. To configure the parameter, run the **11.1.194 low-temperature threshold** command.
AP CPU usage threshold(%)	CPU usage alarm threshold of an AP. To configure the parameter, run the **11.1.79 cpu-usage threshold** command.

Item	Description
AP memory usage threshold(%)	Memory usage alarm threshold of an AP. To configure the parameter, run the **11.1.197 memory-usage threshold** command.
Alarm restriction	Alarm suppression status of an AP. To configure the parameter, run the **11.1.12 alarm-restriction disable** command.
Alarm restriction period(s)	Alarm suppression period of an AP. To configure the parameter, run the **11.1.13 alarm-restriction period** command.
Log server IP address	IP address of the log server. To configure the parameter, run the **11.1.193 log-server** command.
Log record level	Level of AP logs to be backed up. To configure the parameter, run the **11.1.192 log-record-level** command.
Ethernet port MTU(byte)	MTU of Ethernet interfaces. To configure the parameter, run the **11.1.198 mtu** command.
Telnet	Whether AP Telnet login is enabled. To configure the parameter, run the **11.1.266 telnet enable** command.
STelnet server	STelnet server status of an AP. To configure the parameter, run the **11.1.263 stelnet server disable** command.
SFTP server	SFTP server status of an AP. To configure the parameter, run the **11.1.247 sftp server disable** command.
Console	Whether AP console port login is enabled. To configure the parameter, run the **11.1.74 console disable** command.

Item	Description
Antenna output mode	Output mode of the AP's 2.4 GHz or 5 GHz antenna. To configure the parameter, run the **11.10.2 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.
Report disassoc request	Whether an AP is enabled to report disassociation request packets of STAs to the AC. To configure the parameter, run the **11.1.228 report-disassoc-request disable** command.
Sample time(s)	AP's sampling interval. To configure the parameter, run the **11.1.244 sample-time** command.
Dynamic blacklist aging time(s)	Aging time of a dynamic blacklist entry. To configure the parameter, run the **11.7.37 dynamic-blacklist aging-time** command.
MPP active reselection	Active MPP reselection. To configure the parameter, run the **11.9.24 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 set the mode in which an AP reports spectrum data, run the **11.3.7 spectrum-analysis server** command.
Server IP	IP address of the spectrum server. To set the IP address of the spectrum server, run the **11.3.7 spectrum-analysis server** command.

Item	Description
Server port	Port number (UDP port number) of the spectrum server. To set the port number (UDP port number) of the spectrum server, run the **11.3.7 spectrum-analysis server** command.
AC port	Port number used by the AC to receive spectrum data (in UDP packets) from the AP. To set the port number, run the **11.3.7 spectrum-analysis server** command.
Device aging-time(minute)	Aging time of non-Wi-Fi device data on an AC. To set the aging time, run the **11.3.6 spectrum-analysis non-wifi-device aging-time** command.
PoE max power(mW)	Maximum output power of the central AP. To configure the parameter, run the **11.1.207 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 the parameter, run the **11.1.208 poe power-reserved (AP system profile view)** command.
PoE power threshold(%)	Alarm threshold of PoE power consumption percentage on the central AP. To configure the parameter, run the **11.1.209 poe power-threshold (AP system profile view)** command.
PoE af inrush	PoE standard of the central AP. To configure the parameter, run the **11.1.202 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 the parameter, run the **11.1.205 poe high-inrush enable (AP system profile view)** command.

Item	Description
Group address start	Start multicast group address. To configure the parameter, run the **11.12.3 igmp-snooping group-bandwidth (AP system profile view)** command.
Group address end	End multicast group address. To configure the parameter, run the **11.12.3 igmp-snooping group-bandwidth (AP system profile view)** command.
Bandwidth(kbps)	Bandwidth of global multicast groups on an AP. To configure the parameter, run the **11.12.3 igmp-snooping group-bandwidth (AP system profile view)** command.
USB	USB status. To configure the parameter, run the **11.1.278 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 **11.1.252 ssh client first-time enable (AP system profile view)** command.
User interface vty X	VTY user interface *X*. The value of *X* ranges from 0 to 4.
Idle timeout	Timeout period of user connections. To configure this parameter, run the **11.1.279 user-interface vty idle-timeout** command.
Screen length	Number of lines on each terminal screen. To configure this parameter, run the **11.1.280 user-interface vty screen-length** command.
AC protect link switch mode	Active/standby link switchover mode. To configure the parameter, run the **11.13.5 ac protect link-switch mode** command.

Item	Description
AC protect link switch packet loss echo probe time	Number of Echo probe packets sent within a statistics collection interval. To configure the parameter, run the **11.13.4 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 the parameter, run the **11.13.6 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 the parameter, run the **11.13.6 ac protect link-switch packet-loss** command.

Related Topics

11.1.49 ap-system-profile (WLAN view)

11.1.121 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 supported AP types.	-
id *type-id*	Specifies the AP type ID.	The AP type ID must exist.
type *ap-type*	Specifies the AP type name.	The AP type name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap-type** command to view all AP types supported by the device and information about an AP of the specified type.

Example

# Display all AP types supported by the device.

```
<HUAWEI> display ap-type all
--------------------------------------------------------------------------------
ID    Type
--------------------------------------------------------------------------------
17    AP6010SN-GN
19    AP6010DN-AGN
21    AP6310SN-GN
23    AP6510DN-AGN
25    AP6610DN-AGN
27    AP7110SN-GN
28    AP7110DN-AGN
29    AP5010SN-GN
30    AP5010DN-AGN
31    AP3010DN-AGN
33    AP6510DN-AGN-US
34    AP6610DN-AGN-US
35    AP5030DN
36    AP5130DN
37    AP7030DE
38    AP2010DN
39    AP8130DN
40    AP8030DN
42    AP9330DN
43    AP4030DN
44    AP4130DN
45    AP3030DN
46    AP2030DN
47    AP9131DN
48    AP9132DN
49    AP5030DN-S
50    AP3010DN-V2
51    AP4030DN-E
52    AD9430DN-24
53    AD9430DN-12
54    R230D
55    R240D
56    AP6050DN
57    AP6150DN
58    AP7050DE
59    AP7050DN-E
60    AP4030TN
61    AP4050DN-E
62    AP4050DN-HD
64    AP430-E
65    R250D
66    R250D-E
68    AP1010SN
69    AP2050DN
70    AP2050DN-E
71    AP8130DN-W
73    AP2050DN-S
75    AP4050DN
76    AP4051DN
```

```
77     AP4151DN
78     AP4050DN-S
79     AP4051DN-S
80     AP8050DN
81     AP8150DN
82     AP8050DN-S
83     AD9431DN-24X
84     R450D
85     AP1050DN-S
86     AP4051TN
87     AP6052DN
88     AP7052DN
89     AP7052DE
91     AP7152DN
92     AP8050TN-HD
93     AP8082DN
94     AP8182DN
103    AP100EC
104    AP200EC
105    AP300EC
------------------------------------------------------------------------------
Total: 69
```

Table 11-49 Description of the **display ap-type all** command output

Item	Description
ID	ID of an AP.
Type	Type of an AP.

# Display information about AP type 19.

```
<HUAWEI> display ap-type id 19
------------------------------------------------------------------------------
Type                                  : AP6010DN-AGN
AP wired port number                  : 1
AP wired port 0 type                  : GE
Radio number                          : 2
Radio 0 type                          : 802.11bgn
  Maximal spatial streams             : 2
  Maximal antenna number              : 2
  Maximal VAP number                  : 16
  Antenna gain                        : 4
  Frequency switching                 : N
Radio 1 type                          : 802.11an
  Maximal spatial streams             : 2
  Maximal antenna number              : 2
  Maximal VAP number                  : 16
  Antenna gain                        : 5
  Frequency switching                 : N
  Dual-5G high/low band support       : All band(36~165)
Maximum station number                : 128
AP high temperature threshold(degree C): 102
AP low temperature threshold(degree C) : -13
Outdoor                               : N
BLE                                   : N
Number of IoT cards                   : 0
PMF                                   : Y
Optical module                        : N
Optical module information query      : N
Spectrum analysis                     : Y
Mesh                                  : Y
WDS                                   : Y
```

```
Eth-Trunk                    : N
--------------------------------------------------------------------------------
```

Table 11-50 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.
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.
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 5G antenna gain of an AP2010DN is 2.5 dB, the 5G antenna gain of 3 dB is displayed on the AC.
Frequency switching	Whether the radio frequency can be switched. ● Yes ● No
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 5GHz radio works at a high frequency band. ● All band (36-165): The 5GHz radio works at any frequency band.
Maximum station number	Maximum number of STAs supported by the AP type.

Item	Description
AP high temperature threshold(degree C)	High temperature alarm threshold.
AP low temperature threshold(degree C)	Low temperature alarm threshold.
Outdoor	Type of an AP. ● Y: Outdoor AP ● N: Indoor AP
BLE	Whether Bluetooth is supported. ● Yes ● No
Number of IoT cards	Number of IoT cards.
PMF	Whether PMF is supported. ● Yes ● No
Optical module	Whether the optical module is supported. ● Yes ● No
Optical module information query	Whether optical module information can be queried. ● Yes ● No
Spectrum analysis	Whether spectrum analysis is supported. ● Yes ● No
Mesh	Whether the Mesh function is supported. ● Yes ● No
WDS	Whether the WDS function is supported. ● Yes ● No
Eth-Trunk	Whether the Eth-Trunk is supported. ● Yes ● No

Item	Description
Channel mode switching	Whether channel mode switching is supported. ● Yes ● No
External antenna	Whether external antennas are supported. ● Yes ● No

11.1.122 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                        : vlanif100
 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                          : ******
PSK mandatory match switch              : enable
Message-integrity PSK value             : ******
Message-integrity check switch          : enable
Sensitive-info PSK value                : ******
------------------------------------------------------------
```

Table 11-51 Description of the **display capwap configuration** command output

Item	Description
Source interface	AC's source interface. To configure the parameter, run the **11.1.67 capwap source interface** command.
Echo interval(seconds)	Interval for sending Keepalive packets. To specify the interval for sending Keepalive packets, run the **capwap echo interval** command.
Echo times	Number of times for sending Keepalive packets. If the AC or APs receive no response from each other after the Keepalive packets are sent for the specified number of times, the AC or APs consider that they are disconnected from their peer devices. To specify the number of times for sending Keepalive packets, run the **capwap echo times** command.
Control priority(server to client)	Priority of CAPWAP management packets from an AC to an AP. To configure the priority of CAPWAP management packets from an AC to an AP, run the **capwap control-link-priority local** *priority-value* command.
Control priority(client to server)	Priority of CAPWAP management packets from an AP to an AC. To configure the priority of CAPWAP management packets from an AP to an AC, run the **capwap control-link-priority remote** *priority-value* command.
Control-link DTLS encrypt	Whether CAPWAP control tunnel encryption using DTLS is enabled. To enable CAPWAP control tunnel encryption using DTLS, run the **11.1.59 capwap dtls control-link encrypt** command.

Item	Description
DTLS PSK value	PSK for DTLS encryption. To configure the PSK for DTLS encryption, run the **11.1.60 capwap dtls psk** command.
PSK mandatory match switch	Whether an AP is enabled to perform DTLS sessions with the AC using the default PSK. To enable an AP to perform DTLS sessions with the AC using the default PSK, run the **11.1.61 capwap dtls psk-mandatory-match enable** command.
Message-integrity PSK value	PSK used for checking integrity of CAPWAP packets. To configure the parameter, run the **11.1.64 capwap message-integrity psk** command.
Message-integrity check switch	Whether integrity check of CAPWAP packets is enabled. To configure the parameter, run the **11.1.65 capwap message-integrity check disable** command.
Sensitive-info PSK value	PSK used for encrypting sensitive information. To configure the parameter, run the **11.1.66 capwap sensitive-info psk** command.

Related Topics

11.1.58 capwap control-link-priority

11.1.59 capwap dtls control-link encrypt

11.1.60 capwap dtls psk

11.1.61 capwap dtls psk-mandatory-match enable

11.1.62 capwap echo

11.1.64 capwap message-integrity psk

11.1.66 capwap sensitive-info psk

11.1.123 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* | **reason** *reason* }

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.
ap-id *ap-id*	Displays channel switching records of the AP with a specified ID.	The AP ID must exist.
reason *reason*	Displays records of channel switching caused by a specified reason.	The enumerated values are: ● calibration: channel switching caused by radio calibration ● configuration: channel switching caused by configuration ● dfs: channel switching performed to avoid radar channels ● 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

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command enables you to view 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
Old/New: Old channel/New channel
RfID   : Radio ID
--------------------------------------------------------------------------------------------
AP ID  AP name  RfID      Old/New  Switch reason  Switch time
--------------------------------------------------------------------------------------------
1      L2-4f     0        1/6      wds           11:03:30 2014/9/28
--------------------------------------------------------------------------------------------
Total : 1, printed : 1
```

Table 11-52 Description of the **display channel switch-record all** command output

Item	Description
AP ID	AP ID.
AP name	Name of an AP where channel switching has occurred.
RfID	Radio ID.
Old/New	Channels used before and after 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
Switch time	Time when channel switch 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)
PR  : Pre RSSI (dBm)
CR  : Current RSSI (dBm)
RfID: Radio ID
------------------------------------------------------------------------------------------
AP ID AP name   RfID  PCH/CCH  PBW/CBW  PE/CE   PR/CR    Reason        Time
------------------------------------------------------------------------------------------
0     AP1       0     11/6     80M/40M+ 27/127  -32/-40  Period recheck 19:30:00 2016/04/11
0     AP2       0     6/11     20M/20M  27/127  -40/-48  Bad env        19:21:53 2016/04/11
------------------------------------------------------------------------------------------
Total : 2
```

Table 11-53 Description of the **display channel switch-record calibrate** command output

Item	Description
AP ID	AP ID.

Item	Description
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.
PR/CR	Interference values before and after calibration.
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 interfere ● Global plan: network-wide plan ● AP online: AP online ● AP offline: AP offline ● Unknown: unknown reason
Time	Time when calibration is triggered.

Related Topics

11.1.234 reset channel switch-record

11.1.124 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    fcb6-98f5-ec20 fcb6-98f5-ec20 240D-1  10.1.1.182 R240D nor    0              88cf-9837-98a0
88cf-9837-98a0
2    fcb6-98f5-7280 fcb6-98f5-7280 240D    10.1.1.158 R240D nor    0              88cf-9837-98a0
88cf-9837-98a0
3    fcb6-98f6-0ce0 ap1            default 10.1.1.181 R240D nor    0              88cf-9837-98a0  88cf-9837-98a0
--------------------------------------------------------------------------------------------------------------------
Total: 3
```

Table 11-54 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 11-55 AP state list

AP State	Description	Possible Cause	Handling Suggestion
commit-failed	WLAN service configurations fail to be delivered to an AP after the AP goes online on an AC.	After the 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	WLAN service configurations are being delivered to an AP after the AP goes online on an AC.	After the AP goes online on the AC, WLAN service configurations are being delivered to the AP.	This is a normal state, and no action is required.

AP State	Description	Possible Cause	Handling Suggestion
config	WLAN service configurations are being delivered to an AP when the AP is going online on an AC.	After the 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	WLAN service configurations fail to be delivered to an AP when the AP is going online on an AC.	After the 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	An AP is in upgrade state.	When the 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.	The 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.	Handle the AP online failure. For details, see **AP Online Failure** in the *Troubleshooting Insights*.

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.	The AP has not established a CAPWAP link with the AC, the MAC address and SN of the AP that is added offline are different from the actual ones, or license resources are insufficient.	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 obtain 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**

AP State	Description	Possible Cause	Handling Suggestion
			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 license resources of the AC.
name-conflicted	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	An AP is working properly.	An AP successfully goes online on an AC.	This is a normal state, and no action is required.
standby	The AP is in normal state on the standby AC.	In the HSB, dual-link cold backup, or N+1 backup scenario, if the link between the active and standby ACs is established properly, the AP is in standby state on the standby AC and in normal state on the active AC.	This is a normal state, and no action is required.

AP State	Description	Possible Cause	Handling Suggestion
ver-mismatch	The version of an AP does not match that of an AC on which the AP is to go online.	The versions of the AP and the AC mismatch.	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: **http://support.huawei.com/enterprise** - Carrier technical support website: **http://support.huawei.com**
countryCode-mismatch	The country code of an AP does not match that of the AC on which the AP is about to go online.	The current version of the AP does not support the country code configured on the AC.	The AP does not support the country code. Upgrade the AP or change the country code configured on the AC.
unauthed	The AP is not authenticated.	The AP fails to be authenticated.	Run the **ap-confirm** command to confirm unauthenticated APs and allow them to go online.

11.1.125 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, where H is a hexadecimal number of 1 to 4 digits.
verbose	Displays detailed information of the dynamic entries. If *verbose* is not specified, brief information of the dynamic 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 11-56 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.
Learned-From	Interface on which the MAC address is learned.
Type	Type of a MAC address entry.
AP ID	AP ID.

11.1.126 display mac-address { ap-id | ap-name }

Function

The **display mac-address** { **ap-id** | **ap-name**} command displays all dynamic 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 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 MAC address entries on wired interfaces of the AP with the specified name.	The AP name must exist.

Parameter	Description	Value
interface-type interface-number	Displays dynamic 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

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 MAC address entries on an AP's wired interface, including the MAC addresses and VLANs that the AP learns on specified interfaces.

Example

# Display dynamic 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
-------------------------------------------------------------
1051-7254-5a80 1/-        Ethernet0/0/0       dynamic
-------------------------------------------------------------
Total: 1
```

Table 11-57 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.

Related Topics

11.1.235 reset mac-address { ap-id | ap-name }

11.1.127 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 11-58 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
CRC error alarm             : disable
CRC error high threshold(%): 50
CRC error Low threshold(%) : 20
PoE enable                  : enable
PoE legacy                  : disable
PoE power off time range    : -
PoE priority                : low
PoE force power             : disable
Shutdown switch             : disable
------------------------------------------------------------------------------
```

Table 11-59 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 **11.1.183 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 **11.1.190 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 **11.1.190 lldp tlv-enable (AP wired port link profile view)** command.

Item	Description
System capability	Whether an AP's wired interface is allowed to advertise the System-capability TLV. To configure the parameter, run the **11.1.190 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 **11.1.190 lldp tlv-enable (AP wired port link profile view)** command.
System name	Whether an AP's wired interface is allowed to advertise the System-name TLV. To configure the parameter, run the **11.1.190 lldp tlv-enable (AP wired port link profile view)** command.
802.3 TLV power	Whether an AP's wired port is allowed to advertise the Power via MDI TLV. To configure the parameter, run the **11.1.190 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 port. ● 802.1ab: The 802.3 Power via MDI TLV sent by the port conforms to 802.1ab. ● 802.3at: The 802.3 Power via MDI TLV sent by the port conforms to 802.3at. ● 802.3bt: The 802.3 Power via MDI TLV sent by the port conforms to 802.3bt. ● -: Default value. To configure the parameter, run the **11.1.182 lldp dot3-tlv power (AP wired port link profile view)**command.

Item	Description
Legacy TLV four pair power	Whether an AP's wired port is allowed to advertise Cisco's proprietary TLVs. To configure the parameter, run the **11.1.191 lldp tlv-enable legacy-tlv four-pair-power (AP wired port link profile view)**command.
CRC error alarm	Whether the alarm function for CRC errors is enabled on an AP's wired interface. To configure the parameter, run the **11.1.80 crc-alarm enable** command.
CRC error high threshold(%)	Alarm threshold for CRC errors on an AP's wired interface. To configure the parameter, run the **11.1.80 crc-alarm enable** command.
CRC error Low threshold(%)	Clear alarm threshold for CRC errors on an AP's wired interface. To configure the parameter, run the **11.1.80 crc-alarm enable** command.
PoE enable	Whether the PoE function is enabled on the AP's interfaces. To configure the parameter, run the **11.1.203 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 **11.1.206 poe legacy enable (AP wired port link profile view)** command.
PoE power off time range	PoE power-off time range. To configure the parameter, run the **11.1.210 poe power-off time-range (AP wired port link profile view)** command.
PoE priority	Power priority of PoE interfaces on the AP. To configure the parameter, run the **11.1.211 poe priority (AP wired port link profile view)** command.

Item	Description
PoE force power	Whether forcible PoE power supply is enabled on the AP's interfaces. To configure the parameter, run the **11.1.204 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 **11.1.249 shutdown (AP wired port link profile view)** command.

Related Topics

11.1.80 crc-alarm enable

11.1.183 lldp enable

11.1.190 lldp tlv-enable (AP wired port link profile view)

11.1.212 port-link-profile (WLAN view)

11.1.128 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 name              : -
AP group             : -
AP address mode      : -
IPv4 address         : -
IPv4 mask address    : -
IPv4 gateway address : -
IPv4 AC list         : -
--------------------------------------------------------------------------------
```

Table 11-60 Description of the **display provision-ap parameter-list** command output

Item	Description
AP name	AP name. To set this parameter, run the **11.1.43 ap-name (AP provisioning view)** command.
AP group	Group that an AP joins. To set this parameter, run the **11.1.37 ap-group (AP provisioning view)** command.
AP address mode	Mode in which an AP obtains an IP address. To set this parameter, run the **11.1.9 address-mode (AP provisioning view)** command.
IPv4 address	Static IPv4 address of an AP. To set this parameter, run the **11.1.176 ip-address (AP provisioning view)** command.
IPv4 mask address	Static IPv4 address mask of an AP. To set this parameter, run the **11.1.176 ip-address (AP provisioning view)** command.
IPv4 gateway address	IPv4 address gateway of the AP. To set this parameter, run the **11.1.176 ip-address (AP provisioning view)** command.

Item	Description
IPv4 AC list	AC IPv4 address list of an AP. To set this parameter, run the **11.1.6 ac-list(AP provisioning view)** command.

Related Topics

11.1.6 ac-list(AP provisioning view)

11.1.9 address-mode (AP provisioning view)

11.1.37 ap-group (AP provisioning view)

11.1.43 ap-name (AP provisioning view)

11.1.176 ip-address (AP provisioning view)

11.1.129 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 the **display radio** command to view current working status of an AP radio.

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)
--------------------------------------------------------------------------------
AP ID Name            RfID  Band  Type    ST  CH/BW    CE/ME   STA    CU    WM
--------------------------------------------------------------------------------
1     60de-4474-9640  0     2.4G  bgn     on  6/20M    24/24   0      55%   normal
1     60de-4474-9640  1     5G    an     on  56/20M   25/25   0     3%    normal
--------------------------------------------------------------------------------
Total:2
```

Table 11-61 Description of the **display radio** command output

Item	Description
AP ID	AP ID.
Name	AP name.
RfID	Radio ID of an AP.
Band	Working frequency 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
ST	Working status of an AP radio.
CH/BW	Channel/Bandwidth of an AP radio. This item is displayed as "-" if the radio has no VAP profile bound.

Item	Description
CE/ME	Current power of an AP radio/ Maximum power of an AP radio. This item is displayed as "-" if the radio has no VAP profile bound. **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.
CU	Channel usage. When the working mode of an AP radio is the monitor mode, this parameter is displayed as **-**. ● In the AC+central AP+RU networking: RUs do not proactively report the channel usage to the AC. To query the channel usage of RUs, enable the RU data buffer function on the AC. **NOTE** The **ap data-collection enable** command enables the RU 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 usage to the AC. Therefore, the AC does not need to query the channel usage of APs.
WM	Working mode of an AP radio. ● normal ● monitor ● monitor dual-band-scan: inter-band scanning mode

11.1.130 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                    Reference
------------------------------------------------------------
default                       1
------------------------------------------------------------
Total: 1
```

Table 11-62 Description of the **display radio-2g-profile all** command output

Item	Description
Profile name	Name of a 2G radio profile.

Item	Description
Reference	Number of times a 2G radio profile is referenced.

# 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
HT A-MPDU switch                        : enable
HT A-MPDU length limit                  : 3
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                       : -
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)                      : -
High PER threshold(%)                           : 80
Low PER threshold(%)                            : 20
Training interval(s)                            : auto
Training mpdu num                               : 640
Throughput trigger training threshold (%)       : 10
------------------------------------------------------------
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 11-63 Description of the **display radio-2g-profile name** command output

Item	Description
Radio type	Radio type. To configure this parameter, run the **11.1.223 radio-type (2G radio profile view)** command.
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure this parameter, run the **11.2.50 power auto-adjust enable** command.
Beacon interval(TUs)	Interval at which an AP sends Beacon frames, in TU. To configure this parameter, run the **11.1.56 beacon-interval** command.
Beamforming switch	Whether the beamforming function is enabled. To configure this parameter, run the **11.1.57 beamforming enable** command.
Support short preamble	Whether the short preamble is supported. To configure this parameter, run the **11.1.248 short-preamble disable** command.
Fragmentation threshold(Byte)	Packet fragmentation threshold, in bytes. To configure this parameter, run the **11.1.168 fragmentation-threshold** command.
Channel switch announcement	Whether channel switch announcement is enabled. To configure this parameter, run the **11.1.70 channel-switch announcement disable** command.
Channel switch mode	Channel switch announcement mode. To configure this parameter, run the **11.1.71 channel-switch mode** command.
Guard interval mode	GI mode. To configure this parameter, run the **11.1.170 guard-interval-mode** command.

Item	Description
HT A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure this parameter, run the **11.1.172 ht a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure this parameter, run the **11.1.173 ht a-mpdu max-length-exponent** command.
RTS-CTS-mode	RTS/CTS mode. To configure this parameter, run the **11.1.242 rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure this parameter, run the **11.1.243 rts-cts-threshold** command.
802.11bg basic rate	802.11bg basic rate set. To configure this parameter, run the **11.1.158 dot11bg basic-rate** command.
802.11bg support rate	802.11bg supported rate set. To configure this parameter, run the **11.1.159 dot11bg supported-rate** command.
Multicast rate 2.4G	Multicast rate of wireless packets on the 2.4GHz radio. To configure this parameter, run the **11.1.201 multicast-rate** command.
Interference detect switch	Whether interference detection is enabled. To configure this parameter, run the **11.2.47 interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure this parameter, run the **11.2.46 interference co-channel threshold** command.

Item	Description
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure this parameter, run the **11.2.45 interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure this parameter, run the **11.2.48 interference station threshold** command.
WMM switch	Whether the WMM function is enabled. To configure this parameter, run the **11.5.33 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 **11.5.34 wmm mandatory enable** command.
Auto-off start time	Start time for scheduled VAP auto-off. To configure this parameter, run the **11.1.53 auto-off service** command.
Auto-off end time	End time for scheduled VAP auto-off. To configure this parameter, run the **11.1.53 auto-off service** command.
Wifi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure this parameter, run the **11.1.290 wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure this parameter, run the **11.2.54 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 **11.2.4 air-scan-profile (radio profile view)** command.

Item	Description
Smart-antenna	Status of the smart antenna function. To configure this parameter, run the **11.2.59 smart-antenna { enable | disable }** command.
Agile-antenna-polarization	Status of the self-adaptive polarization for agile antennas. To configure this parameter, run the **11.1.11 agile-antenna-polarization** command.
CCA threshold(dBm)	CCA threshold for APs. To configure this parameter, run the **11.2.24 cca-threshold** command.
High PER threshold(%)	Upper valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **11.2.63 smart-antenna valid-per-scope** command.
Low PER threshold(%)	Lower valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **11.2.63 smart-antenna valid-per-scope** command.
Training interval(s)	Smart antenna training interval. To configure this parameter, run the **11.2.61 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 **11.2.62 smart-antenna training-mpdu-number** command.
Throughput trigger training threshold (%)	Sudden throughput change threshold that triggers smart antenna training. To configure this parameter, run the **11.2.60 smart-antenna throughput-triggered-training** command.
Utmost power switch	Whether a radio is enabled to send packets at maximum power. To configure this parameter, run the **11.1.281 utmost-power disable** command.

Item	Description
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure this parameter, run the **11.5.31 wmm edca-ap** command.
AC_VO	AC_VO packets. To configure this parameter, run the **11.5.31 wmm edca-ap** command.
AC_VI	AC_VI packets. To configure this parameter, run the **11.5.31 wmm edca-ap** command.
AC_BE	AC_BE packets. To configure this parameter, run the **11.5.31 wmm edca-ap** command.
AC_BK	AC_BK packets. To configure this parameter, run the **11.5.31 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 **11.5.31 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 **11.5.31 wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure this parameter, run the **11.5.31 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 **11.5.31 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 **11.5.31 wmm edca-ap** command.

11.1.131 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                  Reference
------------------------------------------------------------
default                       1
------------------------------------------------------------
Total: 1
```

Table 11-64 Description of the **display radio-5g-profile all** command output

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

# 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                 : support
Channel switch mode                         : continue
Guard interval mode                         : normal
HT A-MPDU switch                            : disable
HT A-MPDU length limit                      : 3
VHT A-MPDU length limit                     : 7
VHT A-MSDU switch                           : disable
VHT A-MSDU Max frame number                 : 2
RTS-CTS-mode                                : CTS-TO-SELF
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
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)                     : -
High PER threshold(%)                  : 80
Low PER threshold(%)                   : 20
Training interval(s)                   : auto
Training mpdu num                      : 640
Throughput trigger training threshold (%)       : 10
------------------------------------------------------------
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 11-65 Description of the **display radio-5g-profile name** command output

Item	Description
Radio type	Radio type. To configure this parameter, run the **11.1.224 radio-type (5G radio profile view)** command.
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure this parameter, run the **11.2.50 power auto-adjust enable** command.
Beacon interval(TUs)	Interval at which an AP sends Beacon frames, in TU. To configure this parameter, run the **11.1.56 beacon-interval** command.
Beamforming switch	Whether the beamforming function is enabled. To configure this parameter, run the **11.1.57 beamforming enable** command.
Fragmentation threshold(Byte)	Packet fragmentation threshold, in bytes. To configure this parameter, run the **11.1.168 fragmentation-threshold** command.
Channel switch announcement	Whether channel switch announcement is enabled. To configure this parameter, run the **11.1.70 channel-switch announcement disable** command.

Item	Description
Channel switch mode	Channel switch announcement mode. To configure this parameter, run the **11.1.71 channel-switch mode** command.
Guard interval mode	GI mode. To configure this parameter, run the **11.1.170 guard-interval-mode** command.
HT A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure this parameter, run the **11.1.172 ht a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure this parameter, run the **11.1.173 ht a-mpdu max-length-exponent** command.
VHT A-MPDU length limit	Maximum length of the frame aggregated in A-MSDU mode. To configure this parameter, run the **11.1.284 vht a-mpdu max-length-exponent** command.
VHT A-MSDU switch	Whether to enable the function of sending 802.11 packets in A-MSDU mode. To configure this parameter, run the **11.1.285 vht 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 **11.1.286 vht a-msdu max-frame-num** command.
RTS-CTS-mode	RTS/CTS mode. To configure this parameter, run the **11.1.242 rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure this parameter, run the **11.1.243 rts-cts-threshold** command.

Item	Description
802.11a basic rate	802.11a basic rate set. To configure this parameter, run the **11.1.156 dot11a basic-rate** command.
802.11a support rate	802.11a supported rate set. To configure this parameter, run the **11.1.157 dot11a supported-rate** command.
Multicast rate 5G	Multicast rate of wireless packets on the 5 GHz radio. To configure this parameter, run the **11.1.201 multicast-rate** command.
VHT mcs	Maximum MCS value corresponding to a specific number of 802.11ac spatial streams. To configure this parameter, run the **11.1.287 vht mcs-map** command.
Interference detect switch	Whether interference detection is enabled. To configure this parameter, run the **11.2.47 interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure this parameter, run the **11.2.46 interference co-channel threshold** command.
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure this parameter, run the **11.2.45 interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure this parameter, run the **11.2.48 interference station threshold** command.
WMM switch	Whether the WMM function is enabled. To configure this parameter, run the **11.5.33 wmm disable** command.

Item	Description
Mandatory switch	Whether to allow STAs that do not support WMM to connect to a WMM-enabled AP. To configure this parameter, run the **11.5.34 wmm mandatory enable** command.
Auto-off start time	Start time for scheduled VAP auto-off. To configure this parameter, run the **11.1.53 auto-off service** command.
Auto-off end time	End time for scheduled VAP auto-off. To configure this parameter, run the **11.1.53 auto-off service** command.
WiFi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure this parameter, run the **11.1.290 wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure this parameter, run the **11.2.54 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 **11.2.4 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 **11.1.281 utmost-power disable** command.
Smart-antenna	Status of the smart antenna function. To configure this parameter, run the **11.2.59 smart-antenna { enable | disable }** command.
Agile-antenna-polarization	Status of the self-adaptive polarization for agile antennas. To configure this parameter, run the **11.1.11 agile-antenna-polarization** command.

Item	Description
CCA threshold(dBm)	CCA threshold for APs. To configure this parameter, run the **11.2.24 cca-threshold** command.
High PER threshold(%)	Upper valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **11.2.63 smart-antenna valid-per-scope** command.
Low PER threshold(%)	Lower valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **11.2.63 smart-antenna valid-per-scope** command.
Training interval(s)	Smart antenna training interval. To configure this parameter, run the **11.2.61 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 **11.2.62 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 **11.2.60 smart-antenna throughput-triggered-training** command.
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure this parameter, run the **11.5.31 wmm edca-ap** command.
AC_VO	AC_VO packets. To configure this parameter, run the **11.5.31 wmm edca-ap** command.
AC_VI	AC_VI packets. To configure this parameter, run the **11.5.31 wmm edca-ap** command.
AC_BE	AC_BE packets. To configure this parameter, run the **11.5.31 wmm edca-ap** command.

Item	Description
AC_BK	AC_BK packets. To configure this parameter, run the **11.5.31 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 **11.5.31 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 **11.5.31 wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure this parameter, run the **11.5.31 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 **11.5.31 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 **11.5.31 wmm edca-ap** command.

11.1.132 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                    ap-group1
------------------------------------------------------------------------
Total: 1
```

Table 11-66 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.

Item	Description
Reference name	Name of the profile by which an AP system profile is referenced.

11.1.133 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 11-67 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.

11.1.134 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 11-68 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.

11.1.135 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 11-69 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.
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.

11.1.136 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                hw
------------------------------------------------------------
Total: 2
```

Table 11-70 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.

11.1.137 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 11-71 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.

11.1.138 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 11-72 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.

11.1.139 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 the **display references vlan pool** command to view profiles by which a VLAN pool is referenced.

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 11-73 Description of the **display references vlan pool** command output

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

Item	Description
Reference radio	Radio by which a VLAN pool is referenced. This item is displayed only when a VAP profile is bound to radios of an AP group or an AP, and VLANs in a VLAN pool are configured as service VLANs.
WLAN ID	ID of the WLAN by which a VLAN pool is referenced. This item is displayed only when a VAP profile is bound to radios of an AP group or an AP, and VLANs in a VLAN pool are configured as service VLANs.

Related Topics

11.1.246 service-vlan (VAP profile view)

11.1.140 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: 41
```

Table 11-74 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.

Item	Description
Reference port	Interface by which an AP wired port profile is referenced.

11.1.141 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 11-75 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
Wideband switch       : enable
Channel load mode     : outdoor
------------------------------------------------------------
```

Table 11-76 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 **11.1.77 country-code** command.
2.4G dca channel-set	2.4G radio calibration channel set. To configure the parameter, run the **11.2.26 dca-channel channel-set** command.
5G dca bandwidth	5G radio calibration bandwidth. To configure the parameter, run the **11.2.25 dca-channel bandwidth** command.
5G dca channel-set	5G radio calibration channel set. To configure the parameter, run the **11.2.26 dca-channel channel-set** command.

Item	Description
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 **11.9.29 wideband enable** command.
Channel load mode	Channel load mode. ● outdoor: outdoor mode ● indoor: indoor mode To configure this parameter, run the **11.1.69 channel-load-mode indoor** command.

Related Topics

11.1.77 country-code

11.2.25 dca-channel bandwidth

11.2.26 dca-channel channel-set

11.1.142 display snmp-agent trap feature-name wlan all

Function

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

Format

display snmp-agent trap feature-name wlan all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the trap function of a specified feature is enabled, you can run the **display snmp-agent trap feature-name wlan all** command to check the status of all traps of WLAN. You can use the **11.1.251 snmp-agent trap enable feature-name wlan** command to enable the trap function of WLAN.

Prerequisites

SNMP has been enabled. See **snmp-agent**.

Example

# Display all the traps of the WLAN module.

```
<HUAWEI>display snmp-agent trap feature-name wlan all
------------------------------------------------------------------------------
Feature name: WLAN
Trap number : 121
------------------------------------------------------------------------------
Trap name                         Default switch status   Current switch status
hwApFaultNotify                      on                      on
hwApNormalNotify                     on                      on
hwApTypeNotMatchNotify               on                      on
hwApPingResultNotify                 on                      on
hwApUpdateBeginNotify                on                      on
......
hwApVersionMismatchNotify            on                      on
```

Table 11-77 Description of the display snmp-agent trap feature-name wlan all command output

Item	Specification
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Name of traps.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

11.1.251 snmp-agent trap enable feature-name wlan

11.1.143 display ssid-profile

Function

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

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 an SSID profile.

Example

# Display information about all SSID profiles.

```
<HUAWEI> display ssid-profile all
------------------------------------------------------------
Profile name  Beacon 2.4G/5G rate(Mbps)  Reference  SSID
------------------------------------------------------------
default       1/6                        2          HUAWEI-WLAN
------------------------------------------------------------
Total: 1
```

Table 11-78 Description of the **display ssid-profile all** command output

Item	Description
Profile name	SSID profile name.

Item	Description
Beacon 2.4G/5G rate(Mbps)	Rate at which 2.4 GHz or 5 GHz Beacon frames are sent.
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                          : HUAWEI-WLAN
SSID hide                     : disable
Association timeout(min)      : 5
Max STA number                : 64
Reach max STA SSID hide       : enable
Legacy station                : enable
DTIM interval                 : 1
Beacon 2.4G rate(Mbps)        : 1
Beacon 5G rate(Mbps)          : 6
Deny-broadcast-probe          : disable
Probe-response-retry num      : 1
802.11r                       : disable
  802.11r authentication      : -
  Reassociation timeout (s) : -
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
MU-MIMO                       : disable
MU-MIMO optimize              : disable
QBSS load                     : disable
Single txchain                : disable
Advertise AP name             : disable
------------------------------------------------------------------------------
WMM EDCA client parameters:
------------------------------------------------------------------------------
        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
------------------------------------------------------------------------------
```

Table 11-79 Description of the **display ssid-profile name** command output

Item	Description
Profile ID	ID of an SSID profile.
SSID	SSID name. To configure the parameter, run the **11.1.253 ssid** command.

Item	Description
SSID hide	SSID hiding. To configure the parameter, run the **11.1.254 ssid-hide enable** command.
Association timeout(min)	Association timeout period. To configure the parameter, run the **11.1.52 association-timeout** command.
Max STA number	Maximum number of users. To configure the parameter, run the **11.1.196 max-sta-number (SSID profile view)** command.
Reach max STA SSID hide	Whether to automatically hide SSIDs when the number of users reaches the maximum. To configure the parameter, run the **11.1.225 reach-max-sta hide-ssid disable** command.
Legacy station	Whether to permit access of non-HT STAs. To configure the parameter, run the **11.1.180 legacy-station disable** command.
DTIM interval	DTIM interval. To configure the parameter, run the **11.1.160 dtim-interval** command.
Beacon 2.4G rate(Mbps)	Rate at which 2.4 GHz Beacon frames are sent. To configure the parameter, run the **11.1.54 beacon-2g-rate** command.
Beacon 5G rate(Mbps)	Rate at which 5 GHz Beacon frames are sent. To configure the parameter, run the **11.1.55 beacon-5g-rate** command.
Deny-broadcast-probe	Whether an AP is configured not to respond to broadcast Probe Request frames. To configure the parameter, run the **11.1.82 deny-broadcast-probe enable** command.

Item	Description
Probe-response-retry num	Number of times Probe Response packets are retransmitted. To configure the parameter, run the **11.1.214 probe-response-retry** command.
802.11r	802.11r roaming. To configure the parameter, run the **11.4.7 dot11r enable** command.
802.11r authentication	802.11r authentication mode.
Reassociation timeout (s)	802.11r reassociation timeout interval. To configure the parameter, run the **11.4.7 dot11r enable** 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 the parameter, run the **11.5.19 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 the parameter, run the **11.5.19 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 the parameter, run the **11.5.19 qos car (SSID profile view)** command.
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 the parameter, run the **11.5.19 qos car (SSID profile view)** command.

Item	Description
U-APSD	Whether the U-APSD function is enabled. To configure the parameter, run the **11.1.276 u-apsd enable** command.
Active dull client	Whether the function of preventing terminals from entering energy-saving mode is enabled. To configure the parameter, run the **11.1.7 active-dull-client enable** command.
MU-MIMO	Whether the MU-MIMO function is enabled. To configure the parameter, run the **11.1.199 mu-mimo disable** command.
MU-MIMO optimize	Whether the MU-MIMO optimization function is enabled. To configure the parameter, run the **11.1.200 mu-mimo optimize enable** command.
QBSS load	Whether the QBSS load function is enabled. To configure the parameter, run the **11.1.216 qbss-load enable** command.
Single txchain	Whether to enable the single-antenna transmission mode. To configure the parameter, run the **11.1.250 single-txchain enable** command.
Advertise AP name	Whether Beacon frames are enabled to carry the AP name. To configure the parameter, run the **11.1.10 advertise-ap-name enable** command.
AC_VO	AC_VO packets. To configure the parameter, run the **11.5.32 wmm edca-client (SSID profile view)** command.
AC_VI	AC_VI packets. To configure the parameter, run the **11.5.32 wmm edca-client (SSID profile view)** command.

Item	Description
AC_BE	AC_BE packets. To configure the parameter, run the **11.5.32 wmm edca-client (SSID profile view)** command.
AC_BK	AC_BK packets. To configure the parameter, run the **11.5.32 wmm edca-client (SSID profile view)** command.
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **11.5.32 wmm edca-client (SSID profile view)** command.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **11.5.32 wmm edca-client (SSID profile view)** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure the parameter, run the **11.5.32 wmm edca-client (SSID profile view)** command.
TXOPLimit	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 the parameter, run the **11.5.32 wmm edca-client (SSID profile view)** command.

11.1.144 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 11-80 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.

Item	Description
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.

11.1.145 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 of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays STA access information of 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.
sta-mac *sta-mac-address*	Displays access information about a STA with the specified MAC address.	The STA's MAC address must exist.
vlan *vlan-id*	Displays STA access information about a specified VLAN.	The VLAN ID must exist.
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. Access information about STAs can be filtered based on AP groups, APs, and SSIDs. 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. Access information about wireless users can be filtered based on SSIDs. To view details about user authentication, authorization, and accounting information, run the **display access-user** command.

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
--------------------------------------------------------------------------------------------------------------
14cf-9208-9abf   0     1047-8007-6f80  0/2      2.4G  11n   3/8        -70   10    10.10.10.253 tap1     Normal
--------------------------------------------------------------------------------------------------------------
Total: 1 2.4G: 1 5G: 0
```

Table 11-81 Description of the **display station all** command output

Item	Description
STA MAC	STA's MAC address.
AP ID	AP ID.
Ap name	AP name.
Rf/WLAN	Radio ID/WLAN ID of a VAP.
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 APfrom a STA.
VLAN	VLAN ID of a STA.
IP address	IP address of a STA.
SSID	SSID name.

Item	Description
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.

# Display access information about a specified STA.

```
<HUAWEI> display station sta-mac b878-2eb4-2689
------------------------------------------------------------------------------
Station MAC-address                        : b878-2eb4-2689
Station IP-address                         : 10.10.10.254
                                           : FE80::C87:23F4:A6D:8D03
Station gateway                            : 10.10.10.2
Associated SSID                            : jsldoc
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
  ERP enabled                              : No
  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's RSSI(dBm)                        : -28
Station's radio mode                       : 11n
Station's AP ID                            : 0
Station's AP Name                          : area_3
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                       : dcd2-fc04-b513
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
Station supported band                     : 2.4G/5G
Station support 802.11k                    : Yes
Station support 802.11r                    : Yes
Station support 802.11v                    : No
```

```
Available to trigger roam                : Yes
Is sticky client now                     : No
Trigger aimless roam while sticky        : Yes
Neighbor list:
-----------------------------------------
AP name             RfID  SNR     RCPI
-----------------------------------------
-----------------------------------------
total: 0
U-APSD list:
-----------------------------------------------------
AC-VI          AC-VO         AC-BE         AC-BK
-----------------------------------------------------
not-support  not-support  not-support  not-support
-----------------------------------------------------
-----------------------------------------------------------------------------
```

Table 11-82 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.

Item	Description
ERP enabled	Whether Effective radiated power (ERP) is enabled on a STA to increase the physical-layer transmission speed.
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.
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 a patch is used to fix bugs of atheros owl series chips in WDS scenarios.
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 AMSDU size
Station capabilities	Capabilities of a STA.
Station PMF capabilities	PMF capability of a STA.
Station VHT capabilities	Whether a STA supports 802.11ac.
256QAM capabilities	Whether a STA supports 256QAM.
256QAM capabilities	Whether a STA supports 256QAM.

Item	Description
VHT explicit beamforming capabilities	Whether a STA supports 802.11ac explicit beamforming.
MU-MIMO capabilities	Whether a STA supports MU-MIMO
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 Radio ID	Radio ID of a STA.
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 that the STA associates with.
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. ● 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. **NOTE** The NSS value is displayed for STAs working only in 802.11ac mode or STAs working in 802.11n mode and supporting 256QAM.
Station's Short GI	Whether the STA supports the short GI.
Station's roam state	Roaming state of a STA.
Station supported band	Bandwidth supported by a STA.
Station support 802.11k	Whether a STA supports 802.11k.
Station support 802.11r	Whether a STA supports 802.11r.

Item	Description
Station support 802.11v	Whether a STA supports 802.11v.
Available to trigger roam	Whether a STA can trigger the roaming process.
Is sticky client now	Whether a STA is a sticky terminal.
Trigger aimless roam while sticky	Whether a STA is forced to roam aimlessly.
Neighbor list	Neighboring AP list of a STA.
AP name	Name of a STA's neighboring AP.
RfID	Radio ID of a STA's neighboring AP.
SNR	SNR of a STA's neighboring AP.
RCPI	RCPI of a STA's neighboring AP.
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.

Related Topics

13.1.34 display access-user (All views)

11.1.146 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 **11.1.178 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
-------------------------------------------------------------------------------
286E-D488-B74F   Huawei    0         SSID_MYWLAN
-------------------------------------------------------------------------------
Total: 1
```

Table 11-83 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.

Related Topics

11.1.178 keep-service enable allow new-access

11.1.236 reset station assoc-info ap-offline-record

11.1.147 display station online-fail-record

Function

The **display station online-fail-record** command displays STA online failure records.

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 online failure records of all STAs.	-
ap-name *ap-name*	Displays online failure records of STAs on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays online failure records of STAs 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 STA online failure records 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
Rf/WLAN: Radio ID/WLAN ID
---------------------------------------------------------------------------
STA MAC          AP ID Ap name  Rf/WLAN    Last record time
                 Reason
---------------------------------------------------------------------------
14cf-9202-13dc  0     area_11  0/1        2015-03-11/15:53:18
                 The STA is in the VAP's blacklist.
---------------------------------------------------------------------------
Total stations: 1 Total records: 1
```

Table 11-84 Description of the **display station online-fail-record** command output

Item	Description
Radio ID/WLAN ID	Radio/VAP that the STA fails to connect to.
STA MAC	MAC address of the STA that fails to go online.
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	Time of the STA online failure.
Reason STA	Reason for the STA online failure. For details about STA online failure reasons and handling suggestions, see **Table 11-85**. For troubleshooting methods, see **STAs Fail to Associate with a WLAN**.

Table 11-85 STA online failure reasons and handling suggestions

Reason Why a STA Fails to Go Online	Remarks	Handling Suggestion
STA authentication times out.	-	Reassociate the STA with the network. If the failure persists, contact technical support personnel.
Invalid association request packet.	-	Reassociate the STA with the network. If the failure persists, the STA may be incompatible with the AP. Contact technical support personnel.
The encryption mode is inconsistent on the STA and AP.	-	Ensure that the encryption mode is consistent on the STA and AP.
Authentication fails in the association stage.	-	Reassociate the STA with the network. If the failure persists, contact technical support personnel.
The STA is not authenticated.	-	Reassociate the STA with the network. If the failure persists, contact technical support personnel.
The AP does not support the rate set specified in the association request packet of the STA.	-	Change the basic rate set in the radio profile and reassociate the STA with the network.
The encryption algorithm is inconsistent on the STA and AP.	-	Ensure that the encryption algorithm is consistent on the STA and AP.
Failed to decrypt the challenge packet.	-	Verify that the STA works properly and reassociate the STA with the network. If the failure persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Remarks	Handling Suggestion
Access from legacy STAs is denied.	-	Verify that access from legacy STAs is denied. To allow access from legacy STAs, run the **undo legacy-station disable** command.
The number of STAs exceeds the physical specifications allowed by the AP.	-	Expand the network capacity or retain the current configuration as required.
The WMM capability of the STA and VAP does not match.	-	Check whether the VMM function is enabled in the radio profile or check the WMM configuration on the STA.
STAs have a compatibility issue(Incorrect network type flag carried by STAs).	-	Verify that the STA works properly and reassociate the STA with the network. If the failure persists, contact technical support personnel.
STAs have a compatibility issue(STAs do not support short timeslots).	-	Check whether the STA supports 802.11g.
STAs have a compatibility issue(STAs do not support DFS.)	-	Check whether the STA supports 802.11h.
The number of associated STAs exceeds the maximum allowed by the AC.	The number of associated STAs on the AC exceeds the maximum.	Expand the network capacity or retain the current configuration as required.
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.
The STA is not in the VAP's whitelist.	-	Check whether the STA needs to be added to the VAP's whitelist.

Reason Why a STA Fails to Go Online	Remarks	Handling Suggestion
The STA is in the VAP's blacklist.	-	Check whether the STA needs to be added to the VAP's blacklist.
The STA associates with a heavily loaded radio.	-	Check whether the threshold for load balancing is proper.
The STA is in the dynamic blacklist.	-	Check the attack records and check whether the STA has initiated attacks.
The association or reassociation packet check fails.	-	Reassociate the STA with the network. If the failure persists, contact technical support personnel.
The number of users exceeds the maximum allowed on the VAP	-	Expand the network capacity or run the **max-sta-number** command to increase the maximum number of STAs associated with the VAP.
The STA uses a static IP address.	-	Check whether the STA uses a static IP address. If not required, configure the STA to obtain an IP address dynamically.
The STA's SNR is below the user CAC threshold.	-	Check whether the SNR-based user CAC threshold is proper. To change the threshold, run the **uac client-snr threshold** command. Reassociate the STA with the network. Alternatively, determine the STA location and provide coverage to the location.

Reason Why a STA Fails to Go Online	Remarks	Handling Suggestion
The number of STAs exceeds the UAC threshold of the radio.	The number of associated STAs exceeds the user CAC threshold based on the number of users.	Check whether the user CAC threshold based on the number of users is properly set. If not, modify the threshold by running the **uac client-number threshold** command and reassociate the STA with the network.
The channel utilization of the radio has reached the upper threshold.	-	Check whether the user CAC threshold based on the channel utilization is proper. To change the threshold, run the **uac channel-utilization threshold** command. Reassociate the STA with the radio.
The STA does not send an authentication request before associating with the network.	-	Reassociate the STA with the network. If the failure persists, contact technical support personnel.
The key is incorrect or the STA uses the cached PMK.	-	Ensure that the STA uses the correct key and reassociate the STA with the network. If the failure persists, contact technical support personnel.
Failed to receive the handshake packet (2/4) from the STA.	-	Ensure that the STA uses the correct key and reassociate the STA with the network. If the failure persists, contact technical support personnel.
Failed to receive the handshake packet (4/4) from the STA.	-	Ensure that the STA uses the correct key and reassociate the STA with the network. If the failure persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Remarks	Handling Suggestion
WAPI authentication times out.	-	Check the network quality and reassociate the STA with the network. If the failure persists, contact technical support personnel.
Reauthentication fails.	-	Check the intermediate network connectivity between the AP and AC, and reassociate the STA with the network. If the failure persists, contact technical support personnel.
Authentication fails.	-	Reassociate the STA with the network. If the failure persists, contact technical support personnel.
The authentication request times out.	-	Reassociate the STA with the network. If the failure persists, contact technical support personnel.
Key negotiation fails.	-	Ensure that the STA uses the correct key and reassociate the STA with the network. If the failure 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.

Reason Why a STA Fails to Go Online	Remarks	Handling Suggestion
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.
Key negotiation fails(the key information of the handshake packet is invalid).	-	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
The radio type is inconsistent between the AC and AP.	-	Run the **11.1.91 display ap config-info** command to verify the AP radio configuration.

Related Topics

11.1.238 reset station online-fail-record

11.1.148 display station offline-record

Function

The **display station offline-record** command displays STA 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 STA offline records.	-
ap-name *ap-name*	Displays STA offline records on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays STA offline records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac*	Displays logout 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.

Example

# Display all STA offline records.

```
<HUAWEI> display station offline-record all
Rf/WLAN: Radio ID/WLAN ID
------------------------------------------------------------------------------
STA MAC         AP ID Ap name        Rf/WLAN    Last record time
            Reason
------------------------------------------------------------------------------
14cf-9208-9abf  0     area_1         0/2        2015-09-18/09:38:50
            The VAP goes down because the configuration is modified.
14cf-9202-13dc  1     60de-4474-9640 0/1        2015-09-18/09:28:52
            The VAP goes down because the configuration is modified.
------------------------------------------------------------------------------
Total stations: 2 Total records: 2
```

Table 11-86 Description of the **display station offline-record** command output

Item	Description
STA MAC	MAC address of a STA.
AP ID	AP ID.
Ap name	AP name.
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 11-87**. For troubleshooting methods, see **A STA Goes Offline Unexpectedly**.
Total stations	Total number of STAs.
Total records	Total number of STA offline records.

Table 11-87 Possible reasons and suggestions for STAs to go offline

Reason Why a STA Goes Offline	Suggestion
A STA goes offline properly.	No action is required.
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 change 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 **11.1.98 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.
Failed to synchronize user entries between WMP and eSAP.	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.

Reason Why a STA Goes Offline	Suggestion
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 to modify the configuration as required.
The STA roams out of the device.	No action is required.
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 ACs 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 fails the roaming security check: APs before and after roaming use different security policies.	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: Authorization information fails to be delivered.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA MAC is added to the STA blacklist.	Check whether the STA needs to be added to the blacklist.
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 STA disassociates with the network.	Check whether the user actively goes offline or whether the terminal is faulty.

Reason Why a STA Goes Offline	Suggestion
The STA is deauthenticated.	Check whether the user actively goes offline or whether the terminal is faulty.
The STA ages out.	No action is required.
The VAP goes down because the configuration is modified.	Check whether configuration change records exist in the log.
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.	Rectify the fault and 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 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.
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.
No control entry exists.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The AP goes online again.	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.
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.

Reason Why a STA Goes Offline	Suggestion
Multicast key handshake failure.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
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 aging offline).	Check whether the user actively goes offline or whether the terminal is faulty.
The STA is deauthenticated (delay aging offline).	Check whether the user actively goes offline or whether the terminal is faulty.
The STA ages out (delay aging 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.
RADIUS authentication reject.	Check whether the login user name or password and that on the RADIUS server are the same. If not the same, change them to be the same and reapply for login.

Related Topics

11.1.237 reset station offline-record

11.1.149 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.

Parameter	Description	Value
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 this 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, the number of STAs associated with, disassociated from, and reassociated with the AP is displayed.
- If a STA is specified, the number of packets and packet transmission rate between the STA and an AP are displayed.

Prerequisites

- To view statistics information about a specified STA, ensure that the STA has been associated with an AP.
- To view statistics information about STAs associated with a specified AP, 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
------------------------------------------------------------------------------
 AC link auth successful                                      :0
 AC auth failed because of password error                             :0
 AC auth failed because of invalid calc                          :0
 AC auth failed because of timeout                                :0
 AC auth failed because of being refused                              :0
 AC auth failed because of other reasons                              :0
 Sticky stations detected                                     :0
 Trigger sticky stations roam total                              :0
 Trigger sticky stations roam success                              :0
 Trigger sticky stations roam success rate(%)                         :-
 Unavailable to trigger roam                                     :0
 Online sticky stations                                      :0
 Stations supporting dual band                                    :0
 Online stations                                            :0
    Stations associated with 2.4G band                            :0
    Stations associated with 5G band                         :0
------------------------------------------------------------------------------
```

Table 11-88 Description of the **display station statistics** command output

Item	Description
AC link auth successful	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 auth failed because of password error	Number of authentication failures due to the incorrect password.
AC auth failed because of invalid calc	Number of authentication failures due to the invalid authentication algorithm.
AC auth failed because of timeout	Number of authentication failures due to timeout.
AC auth failed because of being refused	Number of authentication failures due to rejected access to the AC.
AC auth failed because of other reasons	Number of authentication failures due to other reasons.
Sticky stations detected	Number of sticky STAs.
Trigger sticky stations roam total	Total number of the triggered smart roaming times.
Trigger sticky stations roam success	Number of the successfully triggered smart roaming times.
Trigger sticky stations roam success rate(%)	Success rate of triggered smart roaming.
Unavailable to trigger roam	Number of STAs that cannot implement smart roaming on the AC.
Online sticky stations	Number of online sticky STAs.
Stations supporting dual band	Number of STAs that support only dual bands.
Online stations	Number of online STAs.
Stations associated with 2.4G band	Number of STAs associated with the 2.4 GHz band.

Item	Description
Stations associated with 5G band	Number of STAs associated with the 5 GHz band.

# Display statistics information about a STA with MAC address 0025-86aa-0d1c.

```
<HUAWEI> display station statistics sta-mac 0025-86aa-0d1c
------------------------------------------------------------------
  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 11-89 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.
Packets received from the station	Number of packets sent by the STA.
Bytes sent to the station	Number of bytes sent to the STA.
Bytes received from the station	Number of bytes sent by 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 N1-2
-------------------------------------------------------------------------------
  Total stations online time(seconds)                 :2713
  Stations associated with the AP                     :1
  Association request                                 :5
  Successful association request                      :5
  Reject association request                          :0
  Failed association request                          :0
  Reassociation request                               :0
  Successful reassociation request                    :0
  Reject reassociation request                        :0
  Failed reassociation request                        :0
  Disassociations because of users notified           :3
  Disassociations because of users roam                          :0
  Disassociations because of users left without notification          :0
  Disassociations because of other reasons                          :0
  Disassociations because of linkauthfail                         :0
  Authentication request                                      :5
  Deauth request                                           :0
  Stations work in power save mode                               :0
  Stations work in HT mode                                     :1
  Stations work in B mode                                     :0
  Stations work in G mode                                     :0
  Stations work in A mode                                     :0
  Stations work in N mode                                     :1
  Stations work in AC mode                                     :0
  Stations only support 2.4G band                                 :1
  Stations only support 5G band                                  :0
  Stations support dual band                                   :0
      Stations associated with 2.4G band                            :1
      Stations associated with 5G band                             :0
  Band steer success rate(%)                                   :0
  Load balancing status between dual band                           :Balanced
  Detected as sticky clients                                   :0
------------------------------------------------------------------------------
```

Table 11-90 Description of the **display station statistics ap-name** *ap-name* command output

Item	Description
Total stations online time(seconds)	Total online duration of all STAs, in seconds.
Stations associated with the AP	Number of STAs currently associated with the AP, not including the number of STAs in aging status.
Association request	Number of association requests sent to the AP.
Successful association request	Number of successful associations.
Reject association request	Number of association requests denied by the AP.
Failed association request	Number of failed associations.
Reassociation request	Number of reassociation requests sent to the AP.
Successful reassociation request	Number of successful reassociations.
Reject reassociation request	Number of reassociation requests rejected by the AP.
Failed reassociation request	Number of failed reassociations.
Disassociations because of users notified	Number of times STAs are disassociated from the AP because users go offline.

Item	Description
Disassociations because of users roam	Number of times STAs are disassociated from the AP because users roam to other regions.
Disassociations because of users left without notification	Number of times STAs are disassociated from the AP because users go offline abnormally.
Disassociations because of other reasons	Number of times STAs are disassociated from the AP for other reasons.
Disassociations because of linkauthfail	Number of times STAs are disassociated from the AP due to link authentication failures.
Authentication request	Number of link authentication request times.
Deauth request	Number of disassociation times.
Stations work in power save mode	Number of STAs working in power saving mode.
Stations work in HT mode	Number of STAs working in HT mode.
Stations work in B mode	Number of STAs working in 802.11b mode.
Stations work in G mode	Number of STAs working in 802.11g mode.
Stations work in A mode	Number of STAs working in 802.11a mode.
Stations work in N mode	Number of STAs working in 802.11n mode.
Stations work in AC mode	Number of STAs working in 802.11ac mode.
Stations only support 2.4G band	Number of STAs that support only the 2.4 GHz frequency band.
Stations only support 5G band	Number of STAs that support only the 5 GHz frequency band.
Stations support dual band	Number of STAs that support both 2.4 and 5 GHz frequency bands.
Stations associated with 2.4G band	Number of STAs that associate with the 2.4 GHz frequency band.
Stations associated with 5G band	Number of STAs that associate with the 5 GHz frequency band.

Item	Description
Band steer success rate(%)	Band steering success rate.
Load balancing status between dual band	Status of load balancing between the 2.4 and 5 GHz frequency bands.

11.1.150 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 of a specified AP radio.	The value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.
ssid *ssid*	Displays information about service VAPs of 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 the **display vap** 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    0023-0024-0080 ON      Open       0     ag
----------------------------------------------------------------------------
Total: 1
```

Table 11-91 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.
Auth type	Authentication mode of a VAP.
STA	Number of terminals connected to a VAP.

11.1.151 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 specified MAC address must exist.
all	Displays records about VAP creation failures on an AP with the specified MAC address.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vap create-fail-record all** 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
------------------------------------------------------------------------------
e468-a350-8a60  0/4      1             ap-group
Service         Preshared key is not configured.
e468-a350-8a60  1/4      1             ap-group
Service         Preshared key is not configured.
e468-a350-8a60  0/6      1             ap-group
Service         Preshared key is not configured.
e468-a350-8a60  1/6      1             ap-group
Service         Preshared key is not configured.
------------------------------------------------------------------------------
Total records: 4
```

Table 11-92 Description of the **display vap create-fail-record all** command output

Item	Description
AP MAC	MAC address of the 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 11-93** describes detailed reasons.

Table 11-93 Reasons for VAP creation failures

Reason for VAP Creation Failures	Remarks
The VAPs using WEP encryption on an AP cannot use the same key ID.	-
Invalid WEP key index.	-
Preshared key is not configured.	-
Only one management VAP profile can be bound.	-
Radio is not exists.	-
VAP already exists.	-
VAP quantity on the Radio reaches the maximum value.	-
The bridge is enable. 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.
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.

Reason for VAP Creation Failures	Remarks
Only one temporary management vap-profile can be bound to an AP.	-
The current country code does not support 5GHz frequency band.	-
The current country code does not support 2.4GHz frequency band.	-
The AP type does not support the wlan id.	-
This AP type does not support WDS function.	-
This AP type does not support Mesh function.	-
The number of VAPs has reached the upper limit.	-
The AP does not support 5GHz frequency band.	-
The AP does not support 2.4GHz frequency band.	-

11.1.152 display vap-profile

Function

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

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 the **display vap-profile** command to view configuration and reference information about a VAP profile.

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 : Beacon 2.4G/5G rate
---------------------------------------------------------------------------------------------------------------
Name         FMode    VLAN    AuthType  STA U/D(Kbps)  VAP U/D(Kbps)  BR2G/5G(Mbps)  Reference  SSID
---------------------------------------------------------------------------------------------------------------
default       direct   VLAN 1  Open      -/-           -/-           1/6          0         HUAWEI-WLAN
vap-profile1  direct   VLAN 1  Open      -/-           -/-           1/6          0         HUAWEI-WLAN
---------------------------------------------------------------------------------------------------------------
Total: 2
```

Table 11-94 Description of the **display vap-profile all** command output

Item	Description
Name	VAP profile name.
FMode	Data forwarding mode.
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(Mbps)	Rate at which 2.4 GHz or 5 GHz Beacon frames are sent.
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                               : -
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
Learn client IPv4 address                : enable
Learn client DHCP strict                 : disable
Learn client DHCP 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
DHCP trust port                          : disable
SFN roam                                 : disable
Anti-attack broadcast-flood              : enable
  Anti-attack broadcast-flood sta-rate-threshold: 10
  Anti-attack broadcast-flood blacklist       : disable
SSID profile                             : default
Security profile                         : default
Traffic profile                          : default
Authentication profile                   :
------------------------------------------------------------------------------
```

Table 11-95 Description of the **display vap-profile name** command output

Item	Description
Profile ID	VAP profile ID.
Service mode	Status of the VAP service. To configure the parameter, run the **11.1.245 service-mode disable** command.
Type	VAP type. ● service: indicates the service type. ● ap-management: indicates the management AP type. To configure the parameter, run the **11.1.275 type (VAP profile view)** command.

Item	Description
Forward mode	Data forwarding mode. - direct-forward: Indicates direct forwarding. - tunnel: Indicates tunnel forwarding. To configure the parameter, run the **11.1.167 forward-mode** command.
Offline management	Whether to enable management VAP and antenna alignment VAP for offline APs. To configure the parameter, run the **11.1.268 temporary-management enable (VAP profile view)** command.
Service VLAN ID	Service VLAN ID. To configure the parameter, run the **11.1.246 service-vlan (VAP profile view)** command.
Service VLAN Pool	VLAN pool to which a service VLAN belongs. To configure the parameter, run the **11.1.246 service-vlan (VAP profile view)** command.
Permit VLAN ID	VLAN from which packets are allowed to pass through after when the authorization VLAN verification function is enabled.
Auto off service switch	Status of the scheduled VAP auto-off function. To configure the parameter, run the **11.1.53 auto-off service** command.
Auto off starttime	Start time for scheduled VAP auto-off. To configure the parameter, run the **11.1.53 auto-off service** command.
Auto off endtime	End time for scheduled VAP auto-off. To configure the parameter, run the **11.1.53 auto-off service** command.
STA access mode	STA access control mode. To configure the parameter, run the **11.7.62 sta-access-mode** command.
STA blacklist profile	STA blacklist profile. To configure the parameter, run the **11.7.62 sta-access-mode** command.

Item	Description
STA whitelist profile	STA whitelist profile. To configure the parameter, run the **11.7.62 sta-access-mode** command.
Band steer	Status of the band steering function. To configure the parameter, run the **11.2.9 band-steer disable** command.
Sta network detect	Whether to forcibly disconnect STAs without traffic. To configure the parameter, run the **11.1.258 sta-network-detect disable** command.
Learn client IPv4 address	Status of STA IPv4 address learning. To configure the parameter, run the **11.7.44 learn-client-address disable (VAP profile view)** command.
Learn client DHCP strict	Status of strict STA IP address learning through DHCP. To configure the parameter, run the **11.7.43 learn-client-address dhcp-strict** command.
Learn client DHCP blacklist	Whether to add STAs with bogus IP addresses to a dynamic blacklist. To configure the parameter, run the **11.7.43 learn-client-address dhcp-strict** command.
IP source check	Status of IP source guard. To configure the parameter, run the **11.7.42 ip source check user-bind enable** command.
ARP anti-attack check	Status of dynamic ARP probing. To configure the parameter, run the **11.7.5 arp anti-attack check user-bind enable** command.
DHCP option82 insert	Whether to enable an AP to insert the Option 82 field in DHCP packets sent from a STA. To configure the parameter, run the **11.1.84 dhcp option82 insert enable** command.

Item	Description
DHCP option82 remote id format	Format of the remote-ID in the Option 82 field inserted in DHCP packets sent from a STA. To configure the parameter, run the **dhcp option82 remote-id format** command.
DHCP option82 circuit id format	Format of the circuit-ID in the Option 82 field inserted in DHCP packets sent from a STA. To configure the parameter, run the **dhcp option82 circuit-id format** command.
MAC format	Format of the AP MAC address in the Option 82 field. To configure the parameter, run the **11.1.85 dhcp option82 format (vap profile view)** command.
DHCP trust port	Status of the DHCP trusted interface function. To configure the parameter, run the **11.7.12 dhcp trust port** command.
SFN roam	Whether agile distributed SFN roaming is enabled. To configure the parameter, run the **11.4.8 sfn-roam enable** command.
Anti-attack broadcast-flood	Status of broadcast flood attack detection. To configure the parameter, run the **11.7.3 anti-attack broadcast-flood disable** command.
Anti-attack broadcast-flood sta-rate-threshold	Broadcast flood threshold. To configure the parameter, run the **11.7.4 anti-attack broadcast-flood sta-rate-threshold** command.
Anti-attack broadcast-flood blacklist	Status of broadcast flood blacklist. To configure the parameter, run the **11.7.2 anti-attack broadcast-flood blacklist enable** command.

Item	Description
SSID profile	Name of the SSID profile referenced by a VAP profile. To configure the parameter, run the **11.1.256 ssid-profile (VAP profile view)** command.
Security profile	Name of the security profile referenced by a VAP profile. To configure the parameter, run the **11.7.59 security-profile (VAP profile view)** command.
Traffic profile	Name of the traffic profile referenced by a VAP profile. To configure the parameter, run the **11.5.24 traffic-profile (VAP profile view)** command.
Authentication profile	Name of the authentication profile referenced by a VAP profile.

Related Topics

11.1.282 vap-profile (WLAN view)

11.1.153 display vlan pool

Function

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

Format

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

Parameters

Parameter	Description	Value
name *pool-name*	Displays detailed information about a specified VLAN pool.	The VLAN pool must exist.
all	Displays brief information about all VLAN pools.	-

Parameter	Description	Value
verbose	Displays detailed information about all VLAN pools.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vlan pool** command to view configuration information about VLAN pools, which facilitates VLAN pool management and maintenance.

Example

# Display brief configuration information about all VLAN pools.

```
<HUAWEI> display vlan pool all
-------------------------------------------------------------------------------
Name                       Assignment                   VLAN total
-------------------------------------------------------------------------------
pool1                      hash                         2
pool2                      hash                         0
-------------------------------------------------------------------------------
Total: 2
```

# Display detailed configuration information about the VLAN pool **pool1**.

```
<HUAWEI> display vlan pool name pool1
-------------------------------------------------------------------------------
Name       : pool1
Total      : 2
Assignment : hash
VLAN ID    : 2 4
-------------------------------------------------------------------------------
```

Table 11-96 Description of the **display vlan pool** command output

Item	Description
Name	Name of a VLAN pool. To configure the parameter, run the **11.1.288 vlan pool** command.
Assignment	VLAN assignment algorithm in a VLAN pool. To configure the parameter, run the **11.1.51 assignment** command.
VLAN total	Number of VLANs added to a VLAN pool.

Item	Description
Total	Total number of VLAN pools.
VLAN ID	VLANs added to a VLAN pool. To configure the parameter, run the **11.1.289 vlan (VLAN pool view)** command.

Related Topics

11.1.51 assignment

11.1.288 vlan pool

11.1.289 vlan (VLAN pool view)

11.1.154 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 the **display wired-port-profile** 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 11-97 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
IGMP-Snooping switch                         : disable
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           IPv6 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 11-98 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 **11.1.213 port-link-profile (AP wired port profile view)** command.
Description	Interface description. To configure the parameter, run the **11.1.83 description (AP wired port profile view)** command.
STP	STP status on a wired interface. To configure the parameter, run the **11.8.14 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 **11.8.9 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 **11.8.18 vlan (AP wired port profile view)** command.
Port untagged VLAN	VLAN to which a wired interface is added in untagged mode. To configure the parameter, run the **11.8.18 vlan (AP wired port profile view)** command.
Port PVID VLAN	PVID of a wired interface. To configure the parameter, run the **11.8.16 vlan pvid (AP wired port profile view)** command.

Item	Description
User isolate mode	User isolation status on a wired interface. To configure the parameter, run the **11.8.15 user-isolate (AP wired port profile view)** command.
DHCP trust port	Status of the DHCP trusted interface function. To configure the parameter, run the **11.7.12 dhcp trust port** command.
ND trust port	Status of the ND trusted interface function.
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 **11.1.174 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 **11.1.81 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 **11.1.264 stp auto-shutdown enable (AP wired port profile view)** command.
Auto shutdown recovery time	Recovery time of the shutdown port triggered by STP. To configure the parameter, run the **11.1.265 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 **11.1.179 learn-client-address enable (AP wired port profile view)** command.

Item	Description
IGMP-Snooping switch	Whether IGMP snooping is enabled on an AP's wired port.
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 **11.1.272 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 **11.1.272 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 **11.1.272 traffic-optimize (AP wired port profile view)** command.
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

Related Topics

11.1.291 wired-port-profile (WLAN view)

11.1.155 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 11-99 Description of the **display wlan config-errors** command output

Item	Description
Profile	Profile name.
Error	Cause of a configuration error.

11.1.156 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 Mbps, 12 Mbps, and 24 Mbps.

Format

dot11a basic-rate { *dot11a-rate-value* &<1-8> | **all** }

undo dot11a basic-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies an 802.11a basic rate set.	Enumerated type: ● 6: 6 Mbps ● 9: 9 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
all	Supports all basic rates.	-

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The rates specified in the basic rate set must be supported by both the AP and STA; otherwise, the STA cannot associate with the AP. For example, if you configure the basic rate set to contain rates 6 Mbps and 9 Mbps 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.

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.

The basic rate set and supported rate set cannot be empty simultaneously.

Example

# Configure the 802.11a basic rate set to contain rates 6 Mbps and 9 Mbps 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
```

Related Topics

11.1.131 display radio-5g-profile

11.1.157 dot11a supported-rate

11.1.157 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 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps.

Format

dot11a supported-rate { *dot11a-rate-value* &<1-8> | **all** }

undo dot11a supported-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies an 802.11a supported rate set.	Enumerated type: ● 6: 6 Mbps ● 9: 9 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
all	Supports all 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 except the basic rates. The AP and STA can transmit data at all rates specified by 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.

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.

The basic rate set and supported rate set cannot be empty simultaneously.

Example

# Configure the 802.11a supported rate set to contain rates 6 Mbps and 9 Mbps 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
```

Related Topics

11.1.131 display radio-5g-profile

11.1.156 dot11a basic-rate

11.1.158 dot11bg basic-rate

Function

The **dot11bg basic-rate** command configures a basic rate set of the 802.11bg protocol in a 2G radio profile.

The **undo dot11bg basic-rate** command restores the default basic rate set of the 802.11bg protocol in a 2G radio profile.

By default, the basic rate set of the 802.11bg protocol includes rates 1 Mbps and 2 Mbps 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 an 802.11bg basic rate set.	Enumerated type: ● 1: 1 Mbps ● 2: 2 Mbps ● 5: 5.5 Mbps ● 6: 6 Mbps ● 9: 9 Mbps ● 11: 11 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
all	Supports all basic rates.	-

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The rates specified in the basic rate set must be supported by both the AP and STA; otherwise, the STA cannot associate with the AP. For example, if you configure the basic rate set to contain rates 6 Mbps and 9 Mbps 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 802.11bg mode, the STA must support all rates specified by the basic rate set; otherwise, the STA cannot associate with the AP.

Precautions

This configuration applies only to STAs associated with an AP in 802.11bg mode but does not take effect on STAs associated with the AP in other modes.

The basic rate set and supported rate set cannot be empty simultaneously.

Example

# Configure the 802.11bg basic rate set to contain rates 6 Mbps and 9 Mbps 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.159 dot11bg supported-rate

11.1.159 dot11bg supported-rate

Function

The **dot11bg supported-rate** command configures a supported rate set of the 802.11bg protocol in a 2G radio profile.

The **undo dot11bg supported-rate** command restores the default supported rate set of the 802.11bg protocol in a 2G radio profile.

By default, the supported rate set of the 802.11bg protocol in a 2G radio profile includes rates 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps.

Format

dot11bg supported-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg supported-rate

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies an 802.11bg supported rate set.	Enumerated type: ● 1: 1 Mbps ● 2: 2 Mbps ● 5: 5.5 Mbps ● 6: 6 Mbps ● 9: 9 Mbps ● 11: 11 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
all	Supports all 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 except the basic rates. The AP and STA can transmit data at all rates specified by 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

802.11bg mode, the AP and STA select a rate from the basic rate set or supported rate set to transmit packets.

Precautions

This configuration applies only to STAs associated with an AP in 802.11bg mode but does not take effect on STAs associated with the AP in other modes.

The basic rate set and supported rate set cannot be empty simultaneously.

Example

# Configure the 802.11bg supported rate set to contain rates 6 Mbps and 9 Mbps 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.158 dot11bg basic-rate

11.1.160 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 waken up frequently, causing high power consumption.

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
```

Related Topics

11.1.143 display ssid-profile

11.1.161 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

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.162 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.	-
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 four 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.163 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

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 **11.1.164 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.164 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 four 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.165 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. It is the maximum transmit power that the AP radio supports under the current configuration. Run the **display radio** { **ap-name** *ap-name* | **ap-id** *ap-id* } command to check the maximum value.

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

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 **undo calibrate auto-txpower-select disable** command, the transmit power configured by running the **eirp** command does not take effect. The automatically selected transmit power prevails.

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 depending on the following principles:

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 to 30 dBm 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] 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.
```

Related Topics

11.1.91 display ap config-info

11.1.129 display radio

11.1.166 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 an integer, and the value is 0.

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.

Prerequisite

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.

NOTE

This command takes effect only on the AP8130DN-W, AP5030DN, AP5130DN, AP8030DN, AP8050DN, AP8050DN-S, AP8150DN, AP8130DN, AP7030DE, AP9330DN, AD9431DN-24X, AP4051TN, AP6052DN, AP8050TN-HD, AP8082DN, AP8182DN, AP7052DN, AP7152DN, AD9430DN-24, AD9430DN-12, AP4030TN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, and AP7050DN-E.

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
```

Related Topics

11.1.154 display wired-port-profile

11.1.167 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 forwarding mode is direct-forward in the VAP profile.

Format

forward-mode { **direct-forward** | **tunnel** }

undo forward-mode

Parameters

Parameter	Description	Value
direct-forward	Indicates the direct forwarding mode.	-
tunnel	Indicates the tunnel forwarding mode.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **forward-mode** command to configure the forwarding mode in a VAP profile. The forwarding modes of VAP profiles can be different.

Example

# Create the VAP profile **vap1** and set the forwarding mode to tunnel forwarding in the profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] forward-mode tunnel
Warning: This action may cause service interruption. Continue?[Y/N]y
```

Related Topics

11.1.152 display vap-profile

11.1.168 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.169 frequency

Function

(AP group radio view) The **frequency** command sets the working frequency of radios for all APs in an AP group.

(AP group radio view) The **undo frequency** command restores the default working frequency of radios for all APs in an AP group.

(AP radio view) The **frequency** command sets the working frequency of radios for an AP.

(AP radio view) The **undo frequency** command restores the working frequency of the radio on an AP to the working frequency configured in the AP group radio view.

By default, radio 0 works on the 2.4 GHz frequency band, and radio 2 works on the 5 GHz frequency band.

Format

frequency { 2.4g | 5g }

undo frequency

Parameters

None.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Radio 0s of the AP2010DN, AP8130DN-W, , AP6052DN, AP7052DN, AP7152DN, AP8182DN, AP8150DN and AP8130DN support 2.4 GHz and 5 GHz frequency bands but they can work on one frequency band at a time. You can configure the working frequency band of the AP based on the frequency band of STAs.

Precautions

The configuration of the 5 GHz frequency band for radio 0 takes effect only on the AP2010DN, AP4030TN supporting three radios, AP8130DN-W, , AP6052DN, AP7052DN, AP7152DN, AP8182DN, AP8150DN and AP8130DN.

The three radios of the AP4051TN and AP8050TN-HD are fixed. Radio 0 works on the 2.4 GHz frequency band, while radios 1 and 2 work on the 5 GHz frequency band.

In dual-5G scenarios, each 5G radio of the AP6052DN, AP7052DN, AP7152DN, AP8182DN, AP8050TN-HD, and AP4051TN supports only the low-frequency channels (36 to 64) or high-frequency channel (100 to 165).

- On the AP6052DN, AP7052DN, AP7152DN, and AP8182DN, radio 1 works on high-frequency channels, and radio 0 works on low-frequency channels.
- On the AP8050TN-HD and AP4051TN, radio 1 works on high-frequency channels, and radio 2 works on low-frequency channels.

Changing the working frequency 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.

Only the AP4030TN supports three radios.

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

If an AP works in dual-5G mode, the channels of the two 5G radios must be separated by at least one channel.

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

Example

# Set the working frequency to the 5 GHz frequency band 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] 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.170 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 is short.

Format

guard-interval-mode { **short** | **normal** }

undo guard-interval-mode

Parameters

Parameter	Description	Value
short	Sets the GI mode to short GI.	-
normal	Sets the GI mode to normal GI.	-

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. There is an interval between the first and second data receiving or transmission or among multiple transmissions. The interval is called Guard Interval (GI) and can improve the transmission effect.

The GI mode consists of the short interval and common interval. The common interval is 800 ns whereas the short interval is 400 ns. The short interval is applicable to 802.11n and 802.11ac specifications, which can raise the transmission rate of 802.11n and 802.11ac packets.

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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.171 high-temperature threshold

Function

The **high-temperature threshold** command sets the upper temperature alarm threshold for APs.

The **undo high-temperature threshold** command restores the default upper temperature alarm threshold for APs.

Table 11-100 Default upper temperature alarm threshold for APs

AP Model	Default Value (°C)
AP4030DN/AP4050DN-S/AP4051DN/AP4151DN	55
AP4050DN/AP1050DN-S	96
AP5030DN/AP5130DN	87
AP6010SN-GN	85
AP6010DN-AGN	102
AP6310SN-GN	94
AP6510DN-AGN	88
AP6510DN-AGN-US	81
AP6610DN-AGN	104
AP6610DN-AGN-US	100

AP Model	Default Value (°C)
AP7110SN	76
AP7110DN	89
AP7030DE/AP9330DN/AP8050DN/AP8050DN-S/AP8150DN	83
AP8030DN	86
AP8130DN	88
AP9131DN/AP9132DN	84
AD9431DN-24X	71
AD9430DN-24	71
AD9430DN-12	83
R230D/R240D/R250D-E/AP2050DN/AP2050DN-E	40
R450D	96
AP6050DN	86
AP7050DE	88
AP7050DN-E	89
AP4030TN/AP4050DN-E/AP4050DN-HD/AP6150DN	50
R250D	102
AP7052DN/AP7152DN/AP7052DE/AP6052DN/AP4051TN	88
AP7052DE	95
AP8082DN/AP8182DN/AP8050TN-HD	91

NOTE

The AP2010DN, AP2030DN, AP2050DN, AP2050DN-E, AP430-E, AP3010DN-AGN, AP5010SN-GN, AP5010DN-AGN, AP4030DN, AP4050DN-S, AP4051DN, AP4151DN, and AP4130DN do not support this command.

Format

high-temperature threshold *threshold*

undo high-temperature threshold

Parameters

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.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.172 ht a-mpdu disable

Function

The **ht a-mpdu disable** command disables aggregation of MPDUs.

The **undo ht a-mpdu disable** command enables aggregation of MPDUs.

By default, aggregation of MPDUs is enabled.

Format

ht a-mpdu disable

undo ht a-mpdu disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce cost, 802.11n uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

# Disable aggregation of MPDUs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] ht a-mpdu disable
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.173 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.

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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.174 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 ipv4 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.

The AP wired interfaces added to an Eth-trunk interface do 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
```

Related Topics

11.1.154 display wired-port-profile

11.1.175 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 **11.1.9 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 are forwarded at Layer 2 and are independent of IP addresses on an agile distributed WLAN. Therefore, the configuration of a static 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, Telnet.

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
```

11.1.176 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 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 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 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 **11.1.9 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 a static 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, Telnet.

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
```

Related Topics

11.1.73 commit (AP provisioning view)

11.1.128 display provision-ap parameter-list

11.1.177 keep-service enable

Function

The **keep-service enable** command configures the AP to continue providing data services after the CAPWAP link between the AP and AC is disconnected.

The **undo keep-service enable** command restores the default setting.

By default, all services on the AP are interrupted after the CAPWAP link between the AP and AC is disconnected.

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 run the **keep-service enable** command to configure the AP to continue providing data services after the CAPWAP link between the AP and AC is disconnected. The data services then no longer depend on the CAPWAP link, which enhances service forwarding robustness.

Precautions

The command does not take effect on a WDS network.

The offline management VAP function and service holding upon CAPWAP link disconnection are mutually exclusive. When the two functions are configured at the same time, the offline management VAP function cannot take effect.

After this command is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue 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.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.178 keep-service enable allow new-access

Function

The **keep-service enable allow new-access** command enables the APs in fault state to allow access of new STAs.

The **undo keep-service enable** command disables the APs in fault state from allowing access of new STAs.

By default, the APs in fault state are disabled from allowing 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

The networks with low security requirements, which apply to hospitals or warehouses, require that the APs in fault state still allow access of new STAs when link faults occur between the APs and AC. After the **keep-service enable allow new-access** command is run, new STAs can still connect to the APs in fault state when the CAPWAP link between the APs and AC is disconnected.

Prerequisites

Open system, Portal, MAC address, WEP, or WPA/WPA2-PSK authentication is used.

Precautions

The command does not take effect on a WDS network.

After this command is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue 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.

To enable an offline AP to allow access of new STAs using Portal or MAC address authentication, configure the **no-auth** parameter.

Example

# Enable the APs in fault state 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
```

11.1.179 learn-client-address enable (AP wired port profile view)

Function

The **learn-client-address enable** command enables terminal IPv4 address learning on an AP's wired interface.

The **undo learn-client-address enable** command disables terminal IPv4 address learning on an AP's wired interface.

By default, terminal address learning is disabled on an AP's wired interface.

Format

learn-client-address ipv4 enable

undo learn-client-address ipv4 enable

Parameters

Parameter	Description	Value
ipv4	IPv4 address.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After terminal address learning is enabled on an AP's wired interface, if a wired terminal connected to the AP 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

The AP wired interfaces added to an Eth-trunk interface do not support this function.

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 terminal 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
```

Related Topics

11.1.154 display wired-port-profile

11.1.180 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 802.11n/ac STAs. If the non-HT STAs access the wireless network, the data transmission rate of 802.11n/ac STAs will be reduced. To prevent the transmission rate of 802.11n/ac 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 shared key authentication mode configured using the **security wep** [**share-key**] 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.
```

Related Topics

11.1.143 display ssid-profile

11.1.181 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.182 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
```

11.1.183 lldp enable

Function

The **lldp enable** command enables LLDP on AP wired interfaces.

The **undo lldp enable** command disables LLDP on AP wired interfaces.

By default, LLDP is enabled on AP wired interfaces.

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) for an AC to query and determine the link status.

Prerequisite

The LLDP function has been enabled in the WLAN view using the **11.1.19 ap lldp enable** command.

Example

# Enable LLDP on the AP 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
```

Related Topics

11.1.19 ap lldp enable

11.1.127 display port-link-profile

11.1.184 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 smaller 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 smaller 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.186 lldp message-transmission interval (AP system profile view)

11.1.185 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.186 lldp message-transmission interval (AP system profile view)

11.1.186 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 larger 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 larger 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 smaller 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 smaller 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.184 lldp message-transmission delay (AP system profile view)

11.1.187 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 huawei
[HUAWEI-wlan-ap-system-prof-huawei] lldp report enable
```

11.1.188 lldp report-interval

Function

The **lldp report-interval** command sets the interval at which an AP reports LLDP neighbor information to an AC.

The **undo lldp report-interval** command restores the default interval at which an AP reports LLDP neighbor information to an AC.

By default, an AP reports LLDP neighbor information to an AC 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 to an AC. 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.189 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 LLDP operation mode for 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 to the connected AC. Setting the delay in re-enabling LLDP on the AP prevents the AP from frequently reporting LLDP neighboring information to the AC when the LLDP status of the AP frequently changes. This reduces the load on the AC and saves resources.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.190 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.

The **undo lldp tlv-enable** command specifies the types of TLVs that an AP wired interface advertises 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.	-
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, 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
```

Related Topics

11.1.19 ap lldp enable

11.1.183 lldp enable

11.1.191 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 proprietary TLVs.

The **undo lldp tlv-enable legacy-tlv four-pair-power** command prohibits an AP's wired interface from advertising Cisco's proprietary TLVs.

By default, an AP's wired interface advertises Cisco's proprietary 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 proprietary 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 proprietary 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 proprietary 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
```

11.1.192 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.	-
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
```

Related Topics

11.1.120 display ap-system-profile

11.1.193 log-server

Function

The **log-server** command configures the log server IP address in the AP system profile and enables log backup on the AP.

The **undo log-server** command restores the default configurations.

By default, 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*

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.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the command to configure the log server IP address 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 attributes of an AP profile changes configurations of all APs using this profile.

Example

# Set the IP address of the log server to 10.0.0.1 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
```

11.1.194 low-temperature threshold

Function

The **low-temperature threshold** command sets the lower temperature alarm threshold for APs.

The **undo low-temperature threshold** command restores the default lower temperature alarm threshold for APs.

Table 11-101 Default lower temperature alarm threshold for APs

AP Model	Default Value (°C)
AP6010SN-GN/AP6010DN-AGN/AP6310SN-GN/AP7110DN-AGN/AP7110SN-GN/AP9330DN/AP6052DN/AP4051TN/AP7152DN/AP7052DE/AP7052DN	-13
AP6510DN-AGN/AP6610DN-AGN/AP6510DN-AGN-US/AP6610DN-AGN-US/AP8030DN/AP8050DN/AP8050DN-S/AP8150DN/AP8130DN/AP9131DN/AP9132DN/AP8082DN/AP8182DN/AP8050TN-HD	-43
AP5030DN/AP5130DN	-28
AP7030DE	-23
AD9430DN-24/AD9431DN-24X	-3
AD9430DN-12	-13
R230D/R240D/R250D-E/AP2050DN/AP2050DN-E	0
AP6050DN/AP7050DE/AP7050DN-E	-13
AP4030TN/AP4050DN-E/AP4050DN-HD/AP6150DN	-10

AP Model	Default Value (°C)
R450D	-13
R250D	-3

NOTE

The AP2010DN, AP2030DN, AP2050DN, AP2050DN-E, AP430-E, AP3010DN-AGN, AP5010SN-GN, AP5010DN-AGN, AP4030DN, AP4050DN-S, AP4051DN, AP4151DN, and AP4130DN do not support this command.

Format

low-temperature threshold *threshold*

undo low-temperature threshold

Parameters

Parameter	Description	Value
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.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.195 management-vlan

Function

The **management-vlan** command configures CAPWAP packets sent from an AP wired interface to carry a management VLAN tag.

The **undo management-vlan** command cancels the management VLAN configuration for CAPWAP packets sent from an AP wired interface.

By default, CAPWAP packets sent from an AP wired interface do not carry a management VLAN tag.

Format

management-vlan *vlan-id*

undo management-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies a management VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, CAPWAP packets sent from an AP wired interface do not carry a management VLAN tag. In most cases, the access switch interface directly connected to the AP adds the PVID to the CAPWAP packets as the management VLAN ID.

If the PVID of the access device has been used for other purposes (for example, as the default VLAN ID of wired users), the PVID cannot be configured as the management VLAN ID on the access device interface. In this case, configure CAPWAP packets sent from an AP wired interface to carry the management VLAN tag. The AP then adds the management VLAN ID to the CAPWAP packets sent to the AC. You only need to configure the access device to allow the packets carrying the management VLAN ID to pass.

Precautions

The configuration takes effect only after the AP is restarted.

On a Mesh network, ensure that CAPWAP packets sent from all APs carry the same management VLAN. Otherwise, MPs cannot go online.

In the following precautions, packets sent from an AP wired interface refer to CAPWAP packets.

- After the **management-vlan** *vlan-id* command is executed, to configure the AP wired interface to allow packets carrying the management VLAN tag to pass through, run the **vlan tagged** *vlan-id* command to add the AP wired interface to the management VLAN in tagged mode.
- After the **management-vlan** *vlan-id* command is executed, to disable packets sent from the AP wired interface from carrying the management VLAN tag, run the **vlan untagged** *vlan-id* command to add the AP wired interface to the management VLAN in untagged mode.
- After the **management-vlan** *vlan-id* command is executed, to add the management VLAN tag to untagged packets received on the AP wired interface, run the **vlan pvid** *vlan-id* command to set the PVID of the AP wired interface to the management VLAN ID.

Example

# Configure CAPWAP packets sent from an AP 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 rese
t. Continue? [Y/N]:y
```

Related Topics

11.1.120 display ap-system-profile

11.8.16 vlan pvid (AP wired port profile view)

11.8.18 vlan (AP wired port profile view)

11.1.196 max-sta-number (SSID profile view)

Function

The **max-sta-number** command sets the maximum number of successfully associated STAs on a VAP.

The **undo max-sta-number** command restores the default maximum number of successfully associated STAs on a VAP.

By default, a VAP allows for a maximum of 64 successfully associated STAs.

Format

max-sta-number *max-sta-number*

undo max-sta-number

Parameters

Parameter	Description	Value
max-sta-number	Specifies the maximum number of successfully associated STAs on a specified VAP.	The value is an integer that ranges from 1 to 256.

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 the **max-sta-number** command to set a proper maximum number of successfully associated STAs on a VAP.

Configuration Impact

After th **max-sta-number** command is executed, online STAs are forcibly to go offline. 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 successfully associated STAs on a VAP while the **authentication wlan-max-user** *max-user-number* command sets the maximum number of STAs authenticated and allowed to pass through in an authentication profile.

Precautions

The maximum number of successfully associated STAs on a specified VAP refers to the maximum number of successfully associated STAs on a VAP of a single AP.

Example

# Set the maximum number of successfully associated STAs on a 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
```

11.1.197 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, the AP sends an alarm message to the AC, and the AC displays the alarm information.
- When the memory usage of an AP falls below the alarm threshold, the AP sends a clear alarm message to the AC, and the AC displays the clear alarm information.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.198 mtu

Function

The **mtu** command sets the maximum transmission unit (MTU) value for the management VLANIF on an AP.

The **undo mtu** command restores the default MTU value for the management VLANIF on an AP.

By default, the MTU value of the management VLANIF 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.	The value is an integer that ranges from 1500 to 1700, in bytes.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

The MTU value is the maximum size of packets sent and received on the management VLANIF of an AP.

NOTICE

Modifying the attributes of an AP system profile changes configurations of all APs using this profile.

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.

Example

# Set the MTU value of the management VLANIF 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.199 mu-mimo disable

Function

The **mu-mimo disable** command disables MU-MIMO.

The **undo mu-mimo disable** command enables MU-MIMO.

By default, the MU-MIMO 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 MU-MIMO 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.

Precautions

- VAPs of only the AP1050DN-S, R450D, R250D, R250D-E, AP2050DN, AP2050DN-E, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DE, and AP7050DN-E support MU-MIMO on 5 GHz radios.
- 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.
- MU-MIMO is not supported on a Mesh network.

Example

# Enable MU-MIMO 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
```

Related Topics

11.1.287 vht mcs-map

11.1.200 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.

Precautions

VAPs of only the AP1050DN-S, R450D, R250D, R250D-E, AP2050DN, AP2050DN-E, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DE, and AP7050DN-E support MU-MIMO on 5 GHz radios.

Prerequisites

The MU-MIMO function has been enabled using the **undo mu-mimo disable** command.

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
```

11.1.201 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.	Enumerated type. The values are as follows in a 2G radio profile: ● 1: 1 Mbps ● 2: 2 Mbps ● 5: 5.5 Mbps ● 6: 6 Mbps ● 9: 9 Mbps ● 11: 11 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps The values are as follows in a 5G radio profile: ● 6: 6 Mbps ● 9: 9 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps

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 Mbps, 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 Mbps 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.223 radio-type (2G radio profile view)

11.1.202 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.

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 Scenarios

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 **11.1.204 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.
- This command takes effect only on the AP7050DN-E, AP4050DN-E, AP4050DN-HD, AP7052DN, AP7152DN, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

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 802.3 af 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.203 poe disable (AP wired port link profile view)

Function

The **poe disable** command disables the PoE function on an AP's interface.

The **undo poe disable** command enables the PoE function on an AP's interface.

By default, the PoE function is enabled on an AP's interface.

Format

poe disable

undo poe disable

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

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.

This command takes effect only on the AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP2050DN-E, R250D-E, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

Example

# Disable the PoE function 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 disable
```

Related Topics

11.1.127 display port-link-profile

11.1.204 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.

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, do not use this command.

This command takes effect only on the AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP2050DN-E, R250D-E, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

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
```

Related Topics

11.1.127 display port-link-profile

11.1.205 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 configures an interface not to allow high inrush current during power-on.

By default, interfaces do not allow high inrush current during power-on.

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.

This command takes effect only on the AP7050DN-E, AP4050DN-E, AP4050DN-HD, AP7052DN, AP7152DN, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.206 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.

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.

Precautions

This command takes effect only on the AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP2050DN-E, R250D-E, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

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
```

Related Topics

11.1.127 display port-link-profile

11.1.207 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.

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 380000 mW.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

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.

This command takes effect only on the AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP2050DN-E, R250D-E, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.211 poe priority (AP wired port link profile view)

11.1.208 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%.

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 Scenarios

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 **11.1.207 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.

This command takes effect only on the AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP2050DN-E, R250D-E, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.207 poe max-power (AP system profile view)

11.1.209 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%.

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.

Precautions

This command takes effect only on the AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP2050DN-E, R250D-E, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.210 poe power-off time-range (AP wired port link profile view)

Function

The **poe power-off time-range** command makes a configured PoE power-off time range effective on an interface.

The **undo poe power-off time-range** command makes a configured PoE power-off time range ineffective on an interface.

By default, no PoE power-off time range takes effective on an interface.

Format

poe power-off time-range *time-range-name*

undo poe power-off time-range

Parameters

Parameter	Description	Value
time-range-name	Specifies a name for a PoE power-off time range.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word all cannot be specified as a time range name.

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **poe power-off time-range** command to configure a PoE power-off time range on an interface. If the current time is within the specified time range, the PD connected to the interface cannot be powered on.

To cancel a configured PoE power-off time range on an interface, run the **undo poe power-off time-range** command. The time range does not take effect on the PD connected to the interface; however, the configuration of the time range is still saved.

Pre-configuration Tasks

Before running the **poe power-off time-range** command, you must ensure a PoE power-off time range has been configured through running the **time-range** command in the system view.

Precautions

This command takes effect only on the AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP2050DN-E, R250D-E, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

Example

# Set a PoE power-off time range from 10:00 am to 11:00 am.

```
<HUAWEI> system-view
[HUAWEI] time-range PoE 10:00 to 11:00 daily
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] poe power-off time-range PoE
```

Related Topics

11.1.127 display port-link-profile

11.1.211 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**.

Format

poe priority { **critical** | **high** | **low** }

undo poe priority

Parameters

Parameter	Description	Value
critical	Indicates the highest priority.	-
high	Indicates the second highest priority.	-
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.

Precautions

This command takes effect only on the AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP2050DN-E, R250D-E, AD9431DN-24X, AD9430DN-24, and AD9430DN-12.

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
```

Related Topics

11.1.127 display port-link-profile

11.1.212 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 **11.1.213 port-link-profile (AP wired port profile view)** command to bind it to an AP wired port profile and then run the **11.1.292 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]
```

Related Topics

11.1.127 display port-link-profile

11.1.213 port-link-profile (AP wired port profile view)

11.1.213 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 **11.1.212 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
```

Related Topics

11.1.133 display references port-link-profile

11.1.154 display wired-port-profile

11.1.212 port-link-profile (WLAN view)

11.1.214 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
```

Related Topics

11.1.143 display ssid-profile

11.1.215 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]
```

Related Topics

11.1.128 display provision-ap parameter-list

11.1.216 qbss-load enable

Function

The **qbss-load enable** command enables the function of notifying STAs of the AP load status.

The **undo qbss-load enable** command disables the function of notifying STAs of the AP load status.

By default, the function of notifying STA of the AP load 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, APs notify STAs of the AP load status during the STA association. The notified information includes the number of STAs associated with the ratio and channel utilization. STAs choose to associate with the optimal AP based on the AP status, improving air interface performance.

Example

# Enable the function of notifying STAs of the AP load status 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
```

Related Topics

11.1.143 display ssid-profile

11.1.217 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 perform configuration only on radio 0 or radio 1, enter the view of the corresponding radio to configure the radio parameters.

Precautions

After running the **radio** *radio-id* command in the AP group view to enter the radio view, you can perform configurations on all specified radios in the AP group; after running the **radio** *radio-id* command in the AP view to enter the radio view, you can perform configurations on the specified AP radio.

Example

# Display the view of radio 0 on the AP with the ID 0

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] radio 0
[HUAWEI-wlan-radio-0/0]
```

Related Topics

11.1.87 display ap

11.1.218 radio disable

Function

(AP group radio view) The **radio disable** command disables all specified radios in an AP group.

(AP group radio view) The **undo radio disable** command enables all specified radios in an AP group.

(AP radio view) The **radio disable** command disables an AP radio.

(AP radio view) The **undo radio disable** command restores the configuration of a specified radio in an AP to the configuration in the AP group radio view.

By default, all AP radios 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 the AP, coverage hole filling will be triggered after the radio is disabled for 5 minutes, to fill coverage holes left by the disabled radio.

Example

# Disable 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] radio disable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.219 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 2G radio of an AP, but does not take effect on the 5G radio. Create a proper radio profile and apply it in the AP view, AP group view, AP radio view, or AP group radio view. In this way, the AP provides better radio signal transmit and receive capabilities.

Follow-up Procedure

Run the **11.1.220 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 in the AP view, AP group view, AP radio view, or AP group radio view cannot be deleted. To delete the 2G radio profile, unbind it in the AP view, AP group view, AP radio view, or AP group radio view first.

You can run the **11.1.169 frequency** command to change the working mode of an AP radio. Generally, radio 0 of an AP works on the 2.4 GHz frequency band, radio 1 works on the 5 GHz frequency band, and radio 2 of the AP4030TN generally works on the 5 GHz frequency band. Radio 0 of the AP2010DN, AP6052DN, AP7052DN, AP7152DN, AP8182DN, AP4030TN, and AP8130DN can work on either the 2.4 GHz or 5 GHz frequency band. Radio 2 of the AP4030TN can work on either the 2.4 GHz or 5 GHz frequency band.

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]
```

Related Topics

11.1.130 display radio-2g-profile

11.1.221 radio-5g-profile (WLAN view)

11.1.220 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 and AP radio view, but the 2G radio profile **default** is applied to 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** }

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 is an integer that is 0 and 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 **11.1.219 radio-2g-profile (WLAN view)** command, bind it to a 2G 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 2G radios in the AP group or the 2G radio of 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 AP group **group1**.

```
<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 group1
[HUAWEI-wlan-ap-group-group1] radio-2g-profile radio-profile1 radio 0
```

Related Topics

11.1.119 display ap-group

11.1.134 display references radio-2g-profile

11.1.219 radio-2g-profile (WLAN view)

11.1.221 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 5G radio of an AP, but does not take effect on the 2G radio. Create a proper radio profile and apply it in the AP view, AP group view, AP radio view, or AP group radio view. In this way, the AP provides better radio signal transmit and receive capabilities.

Follow-up Procedure

Run the **11.1.222 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.
- The 5G radio profile referenced in the AP view, AP group view, AP radio view, or AP group radio view cannot be deleted. To delete the 5G radio profile, unbind it in the AP view, AP group view, AP radio view, or AP group radio view first.

You can run the **11.1.169 frequency** command to change the working mode of an AP radio. Generally, radio 0 of an AP works on the 2.4 GHz frequency band, radio 1 works on the 5 GHz frequency band, and radio 2 of the AP4030TN generally works on the 5 GHz frequency band. Radio 0 of the AP2010DN, AP6052DN, AP7052DN, AP7152DN, AP8182DN, AP4030TN, and AP8130DN can work on either the 2.4 GHz or 5 GHz frequency band. Radio 2 of the AP4030TN can work on either the 2.4 GHz or 5 GHz frequency band.

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]
```

Related Topics

11.1.131 display radio-5g-profile

11.1.219 radio-2g-profile (WLAN view)

11.1.222 radio-5g-profile

Function

The **radio-5g-profile** command binds a 5G radio profile to a 5G radio.

The **undo radio-5g-profile** command unbinds a 5G radio profile from a 5G radio.

By default, no 5G radio profile is applied in the AP view and AP radio view, but the 5G radio profile **default** is applied to 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** }

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 the radio ID.	The value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.
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 **11.1.221 radio-5g-profile (WLAN view)** command, bind it to a 5G 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 5G radios in the AP group or the 5G radio of 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 AP group **group1**.

```
<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 group1
[HUAWEI-wlan-ap-group-group1] radio-5g-profile radio-profile2 radio 1
```

Related Topics

11.1.119 display ap-group

11.1.135 display references radio-5g-profile

11.1.221 radio-5g-profile (WLAN view)

11.1.223 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 **dot11n**.

Format

radio-type { **dot11b** | **dot11g** | **dot11n** }

undo radio-type

Parameters

Parameter	Description	Value
dot11b	Specifies the 802.11b radio type.	-
dot11g	Specifies the 802.11b/g radio type.	-
dot11n	Specifies the 802.11b/g/n radio type.	-

Views

2G radio profile

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **radio-type** command to set the radio type in a radio profile.

Precautions

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 **80211b**.

When the radio type is set to **dot11b** or **dot11g**, the function of denying access from non-HT STAs becomes invalid.

If WDS- or Mesh-enabled radios are configured not to support 802.11n/ac, the air interface backhaul performance will be degraded.

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 Beacon frames and multicast packets that take effect on the 2 GHz radio of the AP are fixed as 1 Mbps, 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.

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
```

Related Topics

11.1.54 beacon-2g-rate

11.1.130 display radio-2g-profile

11.1.201 multicast-rate

11.1.224 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 **dot11ac**.

Format

radio-type { **dot11a** | **dot11n** | **dot11ac** }

undo radio-type

Parameters

Parameter	Description	Value
dot11a	Specifies the 802.11a radio type.	-
dot11n	Specifies the 802.11a/n radio type.	-
dot11ac	Specifies the 802.11a/n/ac radio type.	-

Views

5G radio profile

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **radio-type** command to set the radio type in a radio profile.

Precautions

When the radio type is set to **dot11a**, the function of denying access from non-HT STAs becomes invalid.

If the configured radio type is not supported by an AP, the actual radio type supported by the AP takes effect. For example, if you set the 802.11ac radio type for an 802.11n AP, the 802.11n radio type takes effect on the AP.

If WDS- or Mesh-enabled radios are configured not to support 802.11n/ac, the air interface backhaul performance will be degraded.

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
```

Related Topics

11.1.131 display radio-5g-profile

11.1.225 reach-max-sta hide-ssid disable

Function

The **reach-max-sta hide-ssid disable** command disables automatic SSID hiding when the number of users reaches the maximum.

The **undo reach-max-sta hide-ssid disable** command enables automatic SSID hiding when the number of users reaches the maximum.

By default, automatic SSID hiding is enabled when the number of users reaches the maximum.

Format

reach-max-sta hide-ssid disable

undo reach-max-sta hide-ssid disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

After automatic SSID hiding is enabled, SSIDs are automatically hidden when the number of users connected to the WLAN reaches the maximum, and SSIDs are unavailable for new 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
```

Related Topics

11.1.143 display ssid-profile

11.1.226 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 **11.1.227 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]
```

Related Topics

11.1.141 display regulatory-domain-profile

11.1.227 regulatory-domain-profile

11.1.227 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 **11.1.226 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: Modifying the country code will clear channel, power and antenna gain configurations of the
radio and reset the AP. Continu
e?[Y/N]:y
```

Related Topics

11.1.119 display ap-group

11.1.136 display references regulatory-domain-profile

11.1.226 regulatory-domain-profile (WLAN view)

11.1.228 report-disassoc-request disable

Function

The **report-disassoc-request disable** command enables an AP to report disassociation request packets of STAs to the AC.

The **undo report-disassoc-request disable** command disables an AP from reporting 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
```

11.1.229 report-sta-assoc enable

Function

The **report-sta-assoc enable** command enables the function of recording successful STA associations in the log.

The **undo report-sta-assoc enable** command disables the function of recording successful STA associations in the log.

By default, this function is disabled.

Format

report-sta-assoc enable

undo report-sta-assoc enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of recording successful STA associations in the log is enabled, successfully associated STAs are recorded in the user log.

Configuration Impact

After this function is enabled, each successfully associated user is logged, and a large number of user logs may be recorded.

Example

# Enable the function of recording successful STA associations in the log.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] report-sta-assoc enable
```

11.1.230 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

After an AC is enabled to report information about STA traffic statistics and online duration on APs, the AC collects and reports the information to the eSight when STAs get offline or roam within the AC, which facilitates data query on the 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.

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
```

11.1.231 reset ap offline-record

Function

The **reset ap offline-record** command clears AP offline records.

Format

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

Parameters

Parameter	Description	Value
all	Clears offline records of all APs.	-
mac *mac-address*	Clears 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 offline records, run this command to clear existing records.

Precautions

The cleared records cannot be restored.

Example

# Clear offline records of all APs.

```
<HUAWEI> reset ap offline-record all
```

Related Topics

11.1.98 display ap offline-record

11.1.232 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.

Precautions

The cleared records cannot be restored.

Example

# Clear online failure records of all APs.

```
<HUAWEI> reset ap online-fail-record all
```

Related Topics

11.1.99 display ap online-fail-record

11.1.233 reset ap unauthorized record

Function

The **reset ap unauthorized record** command clears information about unauthenticated 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 information about unauthenticated APs so that removed APs or unauthenticated APs that are physically disconnected from the AC can be cleared. This facilitates collecting statistics and confirmation of unauthenticated APs.

Precautions

If an AP physically connects to the AC but has not been authenticated, the AP is added in the unauthenticated AP list after you run the **reset ap unauthorized record** command.

Example

# Clear information about unauthenticated APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] reset ap unauthorized record
Warning: Clear unauthorized AP record, continue?[Y/N]:y
```

Related Topics

11.1.110 display ap unauthorized record

11.1.234 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
```

Related Topics

11.1.123 display channel switch-record

11.1.235 reset mac-address { ap-id | ap-name }

Function

The **reset mac-address** { **ap-id** | **ap-name**} command clears all dynamic MAC address entries on 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*	Clears all dynamic MAC address entries on wired interfaces of the AP with the specified ID.	The AP ID must exist.
ap-name *ap-name*	Clears all dynamic MAC address entries on wired interfaces of the AP with the specified name.	The AP name must exist.
interface-type interface-number	Clears dynamic 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

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **reset mac-address** command clears all dynamic MAC address entries on an AP's wired interface.

Example

# Clear dynamic MAC address entries on wired interfaces of the AP with ID 1.

```
<HUAWEI> reset mac-address ap-id 1 ethernet 0
```

Related Topics

11.1.126 display mac-address { ap-id | ap-name }

11.1.236 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 **11.1.178 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
```

Related Topics

11.1.178 keep-service enable allow new-access

11.1.146 display station assoc-info ap-offline-record

11.1.237 reset station offline-record

Function

The **reset station offline-record** command deletes STA 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 all STA offline records.	-
ap-name *ap-name*	Deletes STA offline records on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Deletes STA offline records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac*	Deletes offline records of a specified STA.	The specified STA MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to delete existing STA offline records so that the system can record new STA offline events.

Precautions

The deleted STA offline records cannot be restored.

Example

# Delete all STA offline records.

```
<HUAWEI> reset station offline-record all
```

Related Topics

11.1.148 display station offline-record

11.1.238 reset station online-fail-record

Function

The **reset station online-fail-record** command clears STA online failure records.

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	Clears online failure records of all STAs.	-
ap-name *ap-name*	Clears STA online failure records on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Clears STA online failure records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac-address*	Clears online failure records of the STA with the specified MAC address.	The STA's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-collect records about STA online failures, run this command to clear existing records.

Precautions

The cleared records cannot be restored.

Example

# Clear online failure records of all STAs.

```
<HUAWEI> reset station online-fail-record all
```

Related Topics

11.1.147 display station online-fail-record

11.1.239 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 286e-d488-b74f.

```
<HUAWEI> reset station statistics sta-mac 286e-d488-b74f
```

Related Topics

11.1.149 display station statistics

11.1.240 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 the specified name.	The AP name must exist.
ap-id *ap-id*	Clears statistics about the AP with the specified ID.	The AP ID must exist.
ssid *ssid*	Clears statistics about a specified SSID.	The SSID must exist.

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
```

11.1.241 rf-ping

Function

The **rf-ping** command enables an AC to automatically detect wireless link quality.

Format

rf-ping [**-m** *time* | **-c** *number*] * *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 1000.
-c *number*	Specifies the number of probe data packets sent by the AC.	The value is an integer that ranges from 1 to 1000. The default value is 1.
mac-address	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

Use Scenario

This command allows an AC to automatically detect wireless link quality based on link parameters, including the signal strength, data rate on air port, and delay in packet transmission.

Prerequisites

STAs have been associated with the APs and go online.

Example

# Configure an AC to automatically detect quality of the link between the AP and STA with the MAC address 14cf-9202-13dc.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rf-ping 14cf-9202-13dc
 Tx rate=52.0 Mbps, Reply from 14cf-9202-13dc: RSSI=-58 dBm time < 1 ms
 1 packets transmitted, 1 received, 0% packet loss, time < 1 ms, RSSI -58 dBm
```

Table 11-102 Description of the **rf-ping** command output

Item	Description
Tx rate	Transmission rate.
RSSI	Received signal strength.
time	Packet transmission delay.

11.1.242 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.	-
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, when an AP needs to send data to a STA, the AP sends an RTS packet to all STAs associated with it. After receiving the RTS packet, none of the devices within the AP's coverage area sends data within a specified period. After the destination STA receives the RTS packet, it sends a CTS packet. After receiving the CTS packet, none of the devices within the STA's coverage area sends data within a specified period. Using the rts-cts mode to avoid conflicts requires two packets (RTS and CTS packets), increasing packet overhead.
- In cts-to-self mode, when an AP needs to send data to STAs, it sends a CTS packet with its IP address as the source and destination addresses. Then none of the devices within the AP's coverage area sends data within a specified period. In cts-to-self mode, an AP only needs to send a CTS packet to avoid channel conflicts in most scenarios. 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 packets sent on the network. In some situations, however, a channel conflict may still occur when hidden nodes do not receive the CTS packet from the AP. Therefore, the rts-cts mode is more effective in avoiding channel conflicts than the cts-to-self mode.

To avoid a data transmission failure caused by channel conflicts, run the **rts-cts-mode** command to set the RTS-CTS operation mode in a radio profile according to networking requirements.

Example

# Set the RTS-CTS operation mode to **rts-cts** 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-mode rts-cts
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.243 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 a STA, only the STA that receives a CTS frame can send data, and other STAs have channel conflicts by default and must wait and 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.244 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 that can be viewed using the **display** command at a specified interval.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.245 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 **11.1.53 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 11.1.53 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
```

Related Topics

11.1.150 display vap

11.1.246 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*	Sets the service VLAN of a VAP to a specific VLAN.	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 service VLANs of a VAP, STAs connected to the VAP join different VLANs. The VLAN assignment algorithm can be configured using the **11.1.51 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 VLAN2 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
```

Related Topics

11.1.152 display vap-profile

11.1.247 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.248 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** 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.249 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
```

Related Topics

11.1.127 display port-link-profile

11.1.250 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

The single-antenna transmission mode is supported by the R250D, R250D-E, R450D, AP1050DN-S, AP2050DN, AP2050DN-E, AP4050DN, AP4050DN-S, AP4050DN-E, AP4050DN-HD, AP4051DN, AP4151DN, AP6050DN, AP6150DN, AP7050DE, AP7050DN-E, AP8050DN, AP8050DN-S, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, and AP8150DN.

After the single-antenna transmission mode is enabled in an SSID profile, the receive signal strength 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
```

Related Topics

11.1.143 display ssid-profile

11.1.251 snmp-agent trap enable feature-name wlan

Function

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

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

By default, the trap function is enabled for the WLAN module.

Format

snmp-agent trap enable feature-name wlan [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name wlan [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Specifies the name of a trap.	The value is a string and must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

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

Example

# Enable the hwapfaulttrap trap.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name wlan trap-name hwapfaulttrap
```

11.1.252 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, 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 on the SSH client. When the SSH client accesses the SSH server next time, the saved public key 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
```

11.1.253 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. **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
```

Related Topics

11.1.143 display ssid-profile

11.1.254 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
```

Related Topics

11.1.143 display ssid-profile

11.1.255 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 mainly 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 **11.1.256 ssid-profile (VAP profile view)** command to bind the SSID profile to a VAP profile and run the **11.1.283 vap-profile** command to bind the VAP profile to an AP group, AP, AP radio, or AP group radio so that the SSID profile can take effect.

Precautions

- The SSID profile **default** cannot be deleted.
- The SSID profile referenced by a VAP profile cannot be deleted. To delete the SSID profile, unbind it from the VAP profile first.
- If the VAP profile has been applied to an AP group or an AP, modifying the SSID profile will interrupt services.

Example

# Create an SSID profile **ssid1** and enter the SSID profile view.

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

```
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1]
```

Related Topics

11.1.152 display vap-profile

11.1.256 ssid-profile (VAP profile view)

11.1.256 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 **11.1.255 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
```

Related Topics

11.1.137 display references ssid-profile

11.1.152 display vap-profile

11.1.255 ssid-profile (WLAN view)

11.1.257 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 data packets are forwarded in direct forwarding mode, and 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.
- You are not allowed to configure IPv6 functions 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
```

11.1.258 sta-network-detect disable

Function

The **sta-network-detect disable** command disables the device from monitoring user traffic and forcibly disconnecting STAs without traffic.

The **undo sta-network-detect disable** command enables the device to monitor user traffic and forcibly disconnect STAs without traffic.

By default, the device is enabled to monitor user traffic and forcibly disconnect STAs without traffic.

Format

sta-network-detect disable

undo sta-network-detect disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

After the device is enabled to monitor user traffic and forcibly disconnect STAs without traffic, a STA meeting all the following conditions is forcibly disconnected after reassociation and going online:

- The STA does not send DHCP Request messages or receive ARP Reply packets within 5s after going online.
- The IP address of the STA changes after roaming.
- The STA has only uplink traffic but no downlink traffic.

When you do not require user traffic monitoring or want to prevent STAs from being forcibly disconnected, run the command.

Example

# Enable the device to monitor user traffic and forcibly disconnect STAs without traffic.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] undo sta-network-detect disable
```

11.1.259 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 86400, 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.

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
```

Related Topics

11.1.260 sta-offline-delay enable

11.1.144 display sta-offline-delay configuration

11.1.260 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 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, or MAC address-prioritized Portal authentication mode.

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
```

Related Topics

11.1.144 display sta-offline-delay configuration

11.1.261 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
```

Related Topics

11.1.260 sta-offline-delay enable

11.1.144 display sta-offline-delay configuration

11.1.262 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
```

Related Topics

11.1.260 sta-offline-delay enable

11.1.144 display sta-offline-delay configuration

11.1.263 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.264 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 **11.8.14 stp enable (AP wired port profile view) command.**

Precautions

The AP wired interfaces added to an Eth-trunk interface 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
```

Related Topics

11.1.265 stp auto-shutdown recovery-time (AP wired port profile view)

11.1.154 display wired-port-profile

11.1.265 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 **11.1.264 stp auto-shutdown enable (AP wired port profile view)** command.

Precautions

The AP wired interfaces added to an Eth-trunk interface 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
```

Related Topics

11.1.264 stp auto-shutdown enable (AP wired port profile view)

11.1.154 display wired-port-profile

11.1.266 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.263 stelnet server disable

11.1.267 temporary-management enable (AP system profile view)

Function

The **temporary-management enable** command enables offline management VAP and antenna alignment VAP functions.

The **undo temporary-management enable** command disables offline management VAP and antenna alignment VAP functions.

By default, offline management VAP and antenna alignment VAP functions are disabled.

Format

temporary-management enable

undo temporary-management enable

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 antenna alignment VAP function is enabled for an AP, the AP automatically generates an antenna alignment VAP when it works properly. The default SSID and password of the management VAP are **hw_manage_xxxx**. **xxxx** indicates the last four bits of the AP's MAC address. You can associate the mobile phone on which the CloudCampus APP is installed to the wireless network with SSID **hw_manage_xxxx** and use the phone to receive packets sent by the antenna alignment VAP to obtain RSSI 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.

Precautions

- After the offline management VAP and antenna alignment VAP functions are enabled, the administrator needs to change the SSIDs and passwords of the offline management VAP and antenna alignment VAP. Using the default values brings security threats. Any wireless user may use the default SSIDs and passwords to log in to the offline AP and perform unauthorized operations or receive packets sent by the APP. In actual applications, the maintenance personnel may enable the offline management VAP and antenna alignment VAP functions to facilitate AP maintenance. Using the default offline management VAP and antenna alignment VAP is not recommended. To ensure security, the administrator needs to configure a secure VAP profile, set new SSIDs and passwords, and run the **temporary-management enable** command in the VAP profile view to specify the VAPs generated after the VAP profile is bound to an AP group or AP as the offline management VAP and antenna alignment VAP to replace the default offline management VAP and antenna alignment VAP.
- 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. If you want to use an antenna alignment VAP after the deletion, run the **undo temporary-management enable** and the **temporary-management enable** commands in the AP profile view in succession to create a new antenna alignment VAP.
- 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 the central AP is AD9431DN-24X, STAs log in to RUs through the offline management VAP. If the central AP is not AD9431DN-24X, 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.
- The offline management VAP function and service holding upon CAPWAP link disconnection are mutually exclusive. When the two functions are configured at the same time, the offline management VAP function cannot take effect.
- In offline management VAP scenarios, STA address learning does not take effect.

Example

# Enable the offline management VAP and antenna alignment VAP functions.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] temporary-management enable
```

Related Topics

11.1.120 display ap-system-profile

11.1.268 temporary-management enable (VAP profile view)

11.1.268 temporary-management enable (VAP profile view)

Function

The **temporary-management enable** command configures a VAP as the offline management VAP or antenna alignment VAP.

The **undo temporary-management enable** command restores a VAP to the default setting.

By default, a VAP is a service VAP.

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 **temporary-management enable** command in the AP system profile view, an AP automatically generates a management VAP when it becomes faulty. The default SSID and password of the management VAP are **hw_manage_xxxx**. **xxxx** indicates the last four bits of the AP's MAC address. The maintenance personnel can associate the maintenance device to the default VAP and log in to the AP using Telnet 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 **temporary-management enable** command in the AP system profile view, an AP automatically generates an antenna alignment VAP when it works properly. The default SSID and password of the management VAP are

hw_manage_xxxx. **xxxx** indicates the last four bits 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 security of the offline management VAP and antenna alignment VAP, bind a security profile of a high security level to a VAP profile, set new SSIDs and passwords, configure the VAPs 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

Run the **temporary-management enable** command to enable the offline management VAP and antenna alignment VAP functions in the AP system profile view to make the offline management VAP and antenna alignment VAP in the VAP profile 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 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 cannot be 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.
- The offline management VAP function and service holding upon CAPWAP link disconnection are mutually exclusive. When the two functions are configured at the same time, the offline management VAP function cannot take effect.
- In offline management VAP scenarios, STA address learning does not take effect.

Example

# Configure VAPs generated by 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
```

Related Topics

11.1.120 display ap-system-profile

11.1.267 temporary-management enable (AP system profile view)

11.1.269 temporary-management psk

Function

The **temporary-management psk** command configures the password for an offline management VAP or antenna alignment VAP.

The **undo temporary-management psk** command restores the default password of an offline management VAP or antenna alignment VAP.

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

temporary-management psk *psk-value*

undo temporary-management psk

Parameters

Parameter	Description	Value
psk-value	Specifies the password for an offline management VAP or 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

Using the default password of an offline management VAP or antenna alignment VAP poses security risks. You can run the **temporary-management psk** command to change the default password.

Example

# Configure the password for an offline management VAP as **a1234567**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] temporary-management psk a1234567
```

11.1.270 traffic-filter (AP wired port profile view)

Function

The **traffic-filter** command configures ACL-based IPv4 packet filtering on an AP's wired interface.

The **undo traffic-filter** command cancels the ACL-based IPv4 packet filtering configuration on an AP's wired interface.

By default, ACL-based IPv4 packet filtering is not configured on an AP's wired interface.

Format

traffic-filter { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } **ipv4 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.	-
acl	Filters packets based on the ACL.	-
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031.

Parameter	Description	Value
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, the packets are allowed to pass through.

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 of **ap-group1** 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
```

Related Topics

14.1.5 acl (system view)

14.1.4 acl name

11.1.271 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 acl** { *acl-number* | **name** *acl-name* } { **dot1p** *dot1p-value* | **dscp** *dscp-value* }

undo traffic-remark { **inbound** | **outbound** } **ipv4 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.	-

Parameter	Description	Value
ipv4	Configures priority re-marking for IPv4 packets.	-
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031.
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.
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.

- **14.1.5 acl (system view)**
- **14.1.4 acl 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 **11.1.270 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
```

11.1.272 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.	-
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.

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
```

Related Topics

11.1.154 display wired-port-profile

11.1.273 traffic-optimize broadcast-suppression enable (AP system profile view)

Function

The **traffic-optimize broadcast-suppression enable** command enables rate limit for broadcast and multicast packets on an AP.

The **undo traffic-optimize broadcast-suppression enable** command disables rate limit for broadcast and multicast packets on an AP.

By default, rate limit for broadcast and multicast packets is disabled on an AP.

Format

traffic-optimize broadcast-suppression { **all** | **arp** | **igmp** | **nd** | **other** } **enable**

undo traffic-optimize broadcast-suppression { **all** | **arp** | **igmp** | **nd** | **other** } **enable**

Parameters

Parameter	Description	Value
all	Enables rate limit for all broadcast and multicast packets.	-
arp	Enables rate limit for ARP broadcast packets.	-
igmp	Enables rate limit for IGMP multicast packets.	-
nd	Enables rate limit for ND broadcast packets.	-
other	Enables rate limit for broadcast packets other than ARP and ND broadcast packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

A large number of broadcast or multicast packets on a device occupy many network resources, affecting network services. To ensure normal running of network services, you can limit the rate of broadcast and multicast packets on APs with a proper range.

The default rate threshold of broadcast and multicast packets of an AP is 256 pps. You can also run the **11.1.274 traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command to configure a rate threshold for broadcast and multicast packets, which will override the default rate threshold.

Example

# Enable rate limit 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] traffic-optimize broadcast-suppression arp enable
```

Related Topics

11.1.274 traffic-optimize broadcast-suppression rate-threshold (AP system profile view)

11.1.274 traffic-optimize broadcast-suppression rate-threshold (AP system profile view)

Function

The **traffic-optimize broadcast-suppression rate-threshold** command sets a rate threshold for broadcast and multicast packets on an AP.

The **undo traffic-optimize broadcast-suppression rate-threshold** command restores the default threshold of broadcast and multicast packets on an AP.

The default rate threshold for ARP broadcast packets, ND broadcast packets, IGMP multicast packets, and other types of broadcast packets is 256 pps.

Format

traffic-optimize broadcast-suppression { **arp** | **igmp** | **nd** | **other** } **rate-threshold** *threshold-value*

undo traffic-optimize broadcast-suppression { **arp** | **igmp** | **nd** | **other** } **rate-threshold**

Parameters

Parameter	Description	Value
arp	Specifies ARP broadcast packets.	-
igmp	Specifies IGMP multicast packets.	-
nd	Specifies ND broadcast packets.	-
other	Specifies broadcast packets other than ARP and ND broadcast packets.	-
rate-threshold *threshold-value*	Specifies a rate threshold.	The value is an integer that ranges from 64 to 1024, in pps. The default value is 256.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Before setting a rate threshold for broadcast and multicast packets, run the **11.1.273 traffic-optimize broadcast-suppression enable (AP system profile view)** command to enable rate limit for broadcast and multicast packets.

After you run the **traffic-optimize broadcast-suppression rate-threshold** command to configure a rate threshold for broadcast and multicast packets on an AP, the configured threshold will override the default rate threshold. The actual rate of broadcast and multicast packets will not exceed the configured rate threshold. If a large rate threshold is set, the expected network protection effect is not achieved. If a small rate threshold is set, broadcast and multicast packets may be lost. In most cases, use the default rate threshold unless otherwise specified.

Example

# Set the rate 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] traffic-optimize broadcast-suppression all enable
[HUAWEI-wlan-ap-system-prof-system1] traffic-optimize broadcast-suppression arp rate-threshold 300
```

Related Topics

11.1.273 traffic-optimize broadcast-suppression enable (AP system profile view)

11.1.275 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** }

undo type

Parameters

Parameter	Description	Value
ap-management	Sets the type to AP management.	-
service	Sets the type to service.	-

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.

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.

If the type of a VAP is AP management, the VAP does not support portal, MAC address and 802.1x authentication using an external server.

After the VAP type is set to management AP, change the STA's IP address to 169.254.2.x/24 (except 169.254.2.1, 169.254.2.100 is recommended), so that the STA can access the AP.

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
```

Related Topics

11.1.152 display vap-profile

11.1.276 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
```

Related Topics

11.1.143 display ssid-profile

11.1.277 undo ap

Function

The **undo ap** command deletes APs.

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 the 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.

Parameter	Description	Value
ap-mac *ap-mac*	Deletes the AP with the specified MAC address.	The AP's MAC address must exist.
ap-group *group-name*	Deletes the AP in a specified AP group.	The AP group must exist.
all	Deletes all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

If you do not want a specified AP to go online on the AC, run the command to delete the AP from the AC. After the AP is deleted, the AP goes offline from the AC.

Configuration Impact

Deleting an AP will interrupt services of STAs connected to the AP.

Precautions

If an AP is upgraded, in standby state, or the **ap-ping** command is executed, the AP cannot be deleted.

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
```

Related Topics

11.1.87 display ap

11.1.278 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 USB function is supported only by the R250D-E, AP2050DN, AP2050DN-E, AP4050DN-E, AP4051DN, AP4151DN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP6050DN, AP6150DN, AP7050DE, and AP7050DN-E.

Format

usb enable

undo usb enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When users need to save or transfer files using the USB interface provided on some APs, the USB function can be enabled using the **usb enable** command. 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

Some AP functions may be affected after the USB function is enabled.

- The 2.4 GHz radio on the AP6150DN, AP6050DN, AP7050DE, and AP7050DN-E supports only dual spatial streams at most.
- The AP4050DN-E cannot provide PoE power supply.
- The USB function does not take effect when the R250D-E, AP2050DN, and AP2050DN-E use the IEEE 802.3af PoE for power supply.

The affected AP functions are restored after the USB function is disabled.

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
```

Related Topics

11.1.120 display ap-system-profile

11.1.279 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 screen-length** 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 huawei
[HUAWEI-wlan-ap-system-prof-huawei] user-interface vty 0 idle-timeout 1 30
```

11.1.280 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 huawei
[HUAWEI-wlan-ap-system-prof-huawei] user-interface vty 0 screen-length 30
```

11.1.281 utmost-power disable

Function

The **utmost-power disable** command disables radios from sending packets at the maximum power.

The **undo utmost-power disable** command enables radios to send packets at the maximum power.

By default, radios are enabled to send packets at the maximum power.

Format

utmost-power disable

undo utmost-power disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is valid only when the country code is CN. You can run the **undo utmost-power disable** command to enable radios to send packets at the maximum power or at the power specified by the country code. After you run the **utmost-power disable** command, radios send packets at the power specified by the country code. When a country code other than CN is configured, radios can send packets only at the power specified by the country code.

Precautions

Only radios of the AD9430DN-24 (including the mapping RUs), AD9430DN-12 (including the mapping RUs), AD9431DN-24X (including the mapping RUs), AP7030DE, AP9330DN, AP2030DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP3010DN-V2 (supporting 802.11ac after being upgraded from a version earlier than V200R008C10SPC300 to V200R008C10SPC300 or a later version), AP4030TN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DN-E, AP7050DE, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP1050DN-S, AP2050DN, AP2050DN-E, AP8130DN-W, AP5030DN, AP5130DN, AP8030DN, AP8130DN, AP4030DN, AP4130DN, AP9131DN, and AP9132DN can send packets at maximum power.

Example

# Disable radios from sending packets at maximum power.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] utmost-power disable
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.282 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 (" ").

Parameter	Description	Value
all	Deletes all VAP profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a radio profile is applied in the AP group view, AP view, AP radio view, or AP group radio view, the AP can transmit and receive radio signals. After a VAP profile is applied in the AP group view, AP view, AP radio view, or AP group radio view, VAPs are generated and 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 **11.1.283 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 a 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]
```

Related Topics

11.1.152 display vap-profile

11.1.283 vap-profile

11.1.283 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** }

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.
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 the AP2010DN and AP2030DN, each radio supports a maximum of eight VAPs. If the value of *wlan-id* exceeds 8, the configuration cannot take effect and the AP cannot generate wireless signals.

Parameter	Description	Value
radio	Specifies a radio.	-
radio-id	Specifies a radio ID.	The value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.
all	Specifies all radios.	-
service-vlan	Specifies a service VLAN.	-
vlan-id *vlan-id*	Specifies a VLAN ID.	The VLAN ID must exist.
vlan-pool *pool-name*	Specifies a VLAN pool name.	The VLAN pool name 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 **11.1.282 vap-profile (WLAN view)** command, bind it to a radio so that the VAP profile can take effect.

In some scenarios, users hop to configure only one VAP for all APs that use different service VLANs. To simplify configuration, you can configure the **service-vlan** parameter to define a service VLAN when binding a VAP profile. A user-defined service VLAN has a higher priority than that 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 it to 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
```

Related Topics

11.1.119 display ap-group

11.1.138 display references vap-profile

11.1.282 vap-profile (WLAN view)

11.1.284 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.

NOTE

Currently, only the AD9430DN-24 (including the mapping RUs), AD9430DN-12 (including the mapping RUs), AD9431DN-24X (including the mapping RUs), AP7030DE, AP9330DN, AP2030DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP3010DN-V2 (supporting 802.11ac after being upgraded from a version earlier than V200R008C10SPC300 to V200R008C10SPC300 or a later version), AP4030TN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DN-E, AP7050DE, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP1050DN-S, AP2050DN, AP2050DN-E, AP8130DN-W, AP5030DN, AP5130DN, AP8030DN, AP8130DN, AP4030DN, AP4130DN, AP9131DN, and AP9132DN support 802.11ac.

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
```

Related Topics

11.1.131 display radio-5g-profile

11.1.285 vht a-msdu enable

Function

The **vht a-msdu enable** command enables the function of sending 802.11 frames in A-MSDU mode.

The **undo vht a-msdu enable** command disables the function of sending 802.11 frames in A-MSDU mode.

By default, the function of sending 802.11 frames in A-MSDU mode is disabled.

NOTE

Currently, only the AD9430DN-24 (including the mapping RUs), AD9430DN-12 (including the mapping RUs), AD9431DN-24X (including the mapping RUs), AP7030DE, AP9330DN, AP2030DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP3010DN-V2 (supporting 802.11ac after being upgraded from a version earlier than V200R008C10SPC300 to V200R008C10SPC300 or a later version), AP4030TN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DN-E, AP7050DE, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP1050DN-S, AP2050DN, AP2050DN-E, AP8130DN-W, AP5030DN, AP5130DN, AP8030DN, AP8130DN, AP4030DN, AP4130DN, AP9131DN, and AP9132DN support 802.11ac.

Format

vht a-msdu enable

undo vht a-msdu enable

Parameters

None

Views

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 only be enabled on the 802.11ac radio.

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] vht a-msdu enable
```

Related Topics

11.1.131 display radio-5g-profile

11.1.286 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.

NOTE

Currently, only the AD9430DN-24 (including the mapping RUs), AD9430DN-12 (including the mapping RUs), AD9431DN-24X (including the mapping RUs), AP7030DE, AP9330DN, AP2030DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP3010DN-V2 (supporting 802.11ac after being upgraded from a version earlier than V200R008C10SPC300 to V200R008C10SPC300 or a later version), AP4030TN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DN-E, AP7050DE, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP1050DN-S, AP2050DN, AP2050DN-E, AP8130DN-W, AP5030DN, AP5130DN, AP8030DN, AP8130DN, AP4030DN, AP4130DN, AP9131DN, and AP9132DN support 802.11ac.

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 ranging 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.

Prerequisite

The function of sending 802.11 frames in A-MSDU mode has been enabled using the **11.1.285 vht a-msdu enable** command.

Precautions

The function of sending 802.11 frames in A-MSDU mode can only be enabled on the 802.11ac radio.

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
```

Related Topics

11.1.285 vht a-msdu enable

11.1.131 display radio-5g-profile

11.1.287 vht mcs-map

Function

The **vht mcs-map** command configures the maximum MCS value corresponding to a specific number of 802.11ac spatial streams in the 5G radio profile.

The **undo vht mcs-map** command restores the default maximum MCS value corresponding to a specific number of 802.11ac spatial streams in the 5G radio profile.

By default, the maximum MCS value of the 802.11 ac radios is 9 in the 5G radio profile.

NOTE

Currently, only the AD9430DN-24 (including the mapping RUs), AD9430DN-12 (including the mapping RUs), AD9431DN-24X (including the mapping RUs), AP7030DE, AP9330DN, AP2030DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP3010DN-V2 (supporting 802.11ac after being upgraded from a version earlier than V200R008C10SPC300 to V200R008C10SPC300 or a later version), AP4030TN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DN-E, AP7050DE, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP1050DN-S, AP2050DN, AP2050DN-E, AP8130DN-W, AP5030DN, AP5130DN, AP8030DN, AP8130DN, AP4030DN, AP4130DN, AP9131DN, and AP9132DN support 802.11ac.

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 number of spatial streams.	The value is an integer ranging from 1 to 4.
max-mcs *max-mcs-value*	Specifies the maximum MCS value corresponding to a specific number of 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 radios depend on the index value of Modulation and Coding Scheme (MCS). A larger MCS value indicates a higher transmission rate.

- If *nss-value* is equal to or larger than the actual number of spatial streams supported by an AP, the maximum MCS value corresponding to all spatial streams of the AP is *max-mcs-value*.
- If *nss-value* is smaller than the actual number of spatial streams supported by an AP, only the maximum MCS value of configured spatial streams is *max-mcs-value*. The maximum MCS value of the other spatial streams does not take effect.

  For example, if *nss-value* is 2, and the AP supports 3 spatial streams. Only the maximum MCS value of spatial stream 1 and spatial stream 2 is *max-mcs-value*, and that of spatial stream 3 does not take effect.

Precautions

This configuration applies only to STAs associated with an AP in 802.11ac mode but does not take effect on STAs associated with the AP in other modes.

- VAPs of only the AP1050DN-S, R450D, R250D, R250D-E, AP2050DN, AP2050DN-E, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP8050DN, AP8050DN-S, AP8150DN, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DE, and AP7050DN-E support MU-MIMO on 5 GHz radios.
- 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.

- MU-MIMO is not supported on a Mesh network.

Example

# Configure the maximum MCS value 8 for 802.11ac radios with two spatial streams in the 5G radio profile.

```
<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
```

Related Topics

11.1.131 display radio-5g-profile

11.1.288 vlan pool

Function

The **vlan pool** command creates a VLAN pool and displays the VLAN pool view, or displays the view of an existing VLAN pool.

The **undo vlan pool** command deletes a VLAN pool.

By default, no VLAN pool is created.

Format

vlan pool *pool-name*

undo vlan pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Specifies the name of a VLAN pool.	The value is a string of 1 to 31 characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Since WLANs provide flexible access modes, STAs may connect to the same WLAN at the office entrance or stadium entrance, and then roam to different APs. If each SSID has only one service VLAN to deliver wireless access to STAs, IP address resources may become insufficient in areas where many STAs access the WLAN, and IP addresses in the other areas are wasted.

After a VLAN pool is created, add multiple VLANs to the VLAN pool and configure the VLANs as service VLANs. In this way, an SSID can use multiple service VLANs to provide wireless access services. STAs are dynamically assigned to VLANs in the VLAN pool, which reduces the number of STAs in each VLAN and also the size of the broadcast domain. Additionally, IP addresses are evenly allocated, preventing IP address waste.

You can also apply the VLAN pool to a user group to plan network segments by user role.

Follow-up Procedure

After a VLAN pool is created, run the **vlan** command to add VLANs to the VLAN pool. Note that these VLANs have been created using the **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command. Otherwise, VLANs in the VLAN pool cannot take effect.

Precautions

- After a VLAN pool is configured to provide service VLANs, VLANs in the VLAN pool cannot be deleted. To delete the VLAN pool, cancel the service VLAN configuration of the VLAN pool.
- In scenarios where a dual-stack address pool is configured, a STA successfully obtains an IP address if the VLAN pool has assigned an IPv4 or IPv6 address to it. In this case, the VLAN pool will not assign a new VLAN to the STA.

Example

# Create the VLAN pool **pool1** and display the VLAN pool view.

```
<HUAWEI> system-view
[HUAWEI] vlan pool pool1
[HUAWEI-vlan-pool-pool1]
```

Related Topics

11.1.153 display vlan pool

11.1.289 vlan (VLAN pool view)

11.1.289 vlan (VLAN pool view)

Function

The **vlan** command adds a VLAN to a VLAN pool.

The **undo vlan** command deletes a VLAN from a VLAN pool.

By default, no VLAN is available in a VLAN pool.

Format

vlan { *start-vlan* [**to** *end-vlan*] } &<1-10>

undo vlan { { *start-vlan* [**to** *end-vlan*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
start-vlan **to** *end-vlan*	Specifies a VLAN ID. *start-vlan* and *end-vlan* determine a VLAN range. *start-vlan* must be smaller than *end-vlan*.	The value is an integer that ranges from 1 to 4094.

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If service VLANs of a VAP are configured as VLANs in a VLAN pool, STAs connected to the VAP are dynamically assigned to VLANs in the VLAN pool. This prevents a large number of STAs from connecting to the same VLAN, resolving the problems of insufficient IP addresses and large broadcast domain.

Precautions

- A maximum of 128 VLANs can be added to a VLAN pool.
- Deleting a VLAN will interrupt services of STAs using the VLAN. Exercise caution when you delete a VLAN.
- A nonexistent VLAN can also be added to a VLAN pool. However, you need to create the VLAN after adding a nonexistent VLAN to a VLAN pool; otherwise, the VLAN does not take effect.

Example

# Add VLANs 9, 12, 13, and 14 to the VLAN pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] vlan pool pool1
[HUAWEI-vlan-pool-pool1] vlan 9 12 to 14
```

Related Topics

11.1.153 display vlan pool

11.1.288 vlan pool

11.1.290 wifi-light

Function

The **wifi-light** command specifies the parameter reflected by the blinking frequency of the Wireless LED on an AP.

The **undo wifi-light** command restores the default parameter reflected by the blinking frequency of the Wireless LED on an AP.

By default,

- If the Mesh function is enabled on the AP, the blinking frequency of the Wireless LED reflects the weakest signal strength of all neighboring APs.
- If WDS is enabled on an AP, the blinking frequency of the Wireless LED reflects the strength of signals received from a WDS AP.
  - If the AP works in leaf mode, the blinking frequency of the Wireless LED reflects the strength of signals received from a middle AP.
  - If the AP works in middle mode, the blinking frequency of the Wireless LED reflects the strength of signals received from a root AP.
  - If the AP works in root mode, the blinking frequency of the Wireless LED 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 LED reflects the service traffic volume on the radio.

NOTE

Only APs having wireless LEDs support this command. To determine whether an AP has the Wireless LED, check the section **Indicator Description** in the *Hardware Installation and Maintenance Guide* 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 LED on an AP to signal strength. When the Wireless LED blinks fast, the signal strength is strong.	-

Parameter	Description	Value
traffic	Sets the parameter reflected by the blinking frequency of the Wireless LED on an AP to service traffic volume. When the Wireless LED 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 an AP that has the WDS or Mesh function enabled, you need to adjust AP locations and antenna directions to obtain strong signals. If the blinking frequency of the Wireless LED 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 LED. 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 LED always shows service traffic volume.

Example

# Set the parameter reflected by the blinking frequency of the Wireless LED 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.1.291 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 **11.1.292 wired-port-profile (AP group view and 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]
```

Related Topics

11.1.154 display wired-port-profile

11.1.292 wired-port-profile (AP group view and view)

11.1.292 wired-port-profile (AP group view and 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 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 **11.1.291 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.

Example

# Create the AP wired port profile **wired-port1** and bind it to GE0 of 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
```

Related Topics

11.1.119 display ap-group

11.1.140 display references wired-port-profile

11.1.291 wired-port-profile (WLAN view)

11.1.293 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 WLAN Radio Resource Management Configuration Commands

11.2.1 Command Support

- Only the S5720HI supports WLAN-AC commands.
- The AP3010DN-AGN, AP5010DN-AGN, AP5010SN-GN, and AP6310SN-GN do not support the high-density function.

11.2.2 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 takes effect only on APs in compliance with 802.11n.

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 huawei
[HUAWEI-wlan-rrm-prof-huawei] amc-policy high-stability
```

Related Topics

11.2.31 display rrm-profile

11.2.3 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 **11.2.28 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 **11.2.4 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]
```

Related Topics

11.2.4 air-scan-profile (radio profile view)

11.2.4 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 **11.2.3 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
```

Related Topics

11.2.3 air-scan-profile

11.2.5 band-steer balance gap-threshold

Function

The **band-steer balance gap-threshold** command sets the load difference threshold for load balancing between radios.

The **undo band-steer balance gap-threshold** command restores the default load difference threshold for load balancing between radios.

By default, the load difference threshold for load balancing between radios is 20%.

Format

band-steer balance gap-threshold *gap-threshold*

undo band-steer balance gap-threshold

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold*	Specifies the load difference threshold for load balancing between radios.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **undo band-steer disable** command to configure the band steering function. If an AP and STAs connected to the AP can work at both 2.4 and

5 GHz radios, the band steering function allows radios of the AP to load balance traffic. This helps minimize interference between STAs and improve user experience.

When a STA requests to connect to an AP radio, the AP enabled with band steering will collect statistics about access users on each radio.

1. If the number of access users on the AP does not exceed **start-threshold** specified using the **11.2.6 band-steer balance start-threshold** command, the STA can preferentially associate with the 5 GHz radio.
2. If the number of access users on the AP exceeds **start-threshold**, the AP determines the frequency band to which the STA connects based on radio load difference computed according to the formula: (Number of access users on the 5 GHz radio – Number of access users on the 2.4 GHz radio)/Number of access users on the 5 GHz radio * 100%.

For example, if a STA requests to associate with the AP at the 2.4 GHz radio but the number of access users on the AP has exceeded **start-threshold**, the AP implements load balancing between the 2.4 GHz and 5 GHz radios according to their load difference. If the value obtained based on the formula (Number of access users on the 5 GHz radio – Number of access users on the 2.4 GHz radio)/ Number of access users on the 5 GHz radio * 100% is greater than **gap-threshold**, the AP preferentially associates with the STA on the 2.4 GHz radio; otherwise, the AP preferentially associates with the STA on the 5 GHz radio.

Example

# Set the load difference threshold to 25% in the RRM profile **huawei**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] band-steer balance gap-threshold 25
```

Related Topics

11.2.8 band-steer deny-threshold

11.2.6 band-steer balance start-threshold

11.2.6 band-steer balance start-threshold

Function

The **band-steer balance start-threshold** command sets the start threshold for load balancing between radios.

The **undo band-steer balance start-threshold** command restores the default start threshold for load balancing between radios.

By default, the start threshold for load balancing between radios 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 load balancing between radios.	The value is an integer that ranges from 0 to 100.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **undo band-steer disable** command to configure the band steering function. If an AP and STAs connected to the AP support both radios, the band steering function allows radios of the AP to load balance traffic. This helps minimize interference between STAs and improve user experience.

When a STA requests to connect to an AP radio, the AP enabled with band steering will collect statistics about access users on each radio.

1. If the number of access users on the AP does not exceed **start-threshold**, the STA can preferentially associate with the 5 GHz radio.
2. If the number of access users on the AP exceeds **start-threshold**, the AP determines the frequency band to which the STA connects based on radio load difference computed according to the formula: (Number of access users on the 5 GHz radio – Number of access users on the 2.4 GHz radio)/Number of access users on the 5 GHz radio * 100%

For example, if a STA requests to associate with the AP at the 2.4 GHz radio but the number of access users on the AP has exceeded **start-threshold**, the AP implements load balancing between the 2.4 GHz and 5 GHz radios according to their load difference. If the value obtained based on the formula (Number of access users on the 5 GHz radio – Number of access users on the 2.4 GHz radio)/ Number of access users on the 5 GHz radio * 100% is greater than **gap-threshold** configured using the **11.2.5 band-steer balance gap-threshold** command, the AP preferentially associates with the STA on the 2.4 GHz radio; otherwise, the AP preferentially associates with the STA on the 5 GHz radio.

Example

# Set the start threshold to 20 in the RRM profile **huawei**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] band-steer balance start-threshold 20
```

Related Topics

11.2.5 band-steer balance gap-threshold

11.2.8 band-steer deny-threshold

11.2.7 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 300.

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 **huawei** 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 huawei
[HUAWEI-wlan-rrm-prof-huawei] band-steer client-band-expire 80
```

11.2.8 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.

Example

# Set the maximum number of rejections to 8 for the terminal **huawei**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] band-steer deny-threshold 8
```

Related Topics

11.2.9 band-steer disable

11.2.9 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 **huawei** 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.

The AP2010DN does not support the band steering function.

Example

# Disable band steering.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name huawei
[HUAWEI-wlan-vap-prof-huawei] band-steer disable
```

Related Topics

11.1.152 display vap-profile

11.2.10 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 5 to 75, 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 **huawei** to 20 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] band-steer snr-threshold 20
```

11.2.11 calibrate auto-channel-select disable

Function

The **calibrate auto-channel-select disable** command disables automatic channel selection.

The **undo calibrate auto-channel-select disable** command enables automatic channel selection.

By default, automatic channel selection is enabled.

Format

calibrate auto-channel-select disable

undo calibrate auto-channel-select disable

Parameters

None

Views

RRM profile 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.

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 in the RRM profile **802.11b**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name 802.11b
[HUAWEI-wlan-rrm-prof-802.11b] calibrate auto-channel-select disable
```

11.2.12 calibrate auto-txpower-select disable

Function

The **calibrate auto-txpower-select disable** command disables automatic transmit power selection.

The **undo calibrate auto-txpower-select disable** command enables automatic transmit power selection.

By default, automatic transmit power selection is enabled.

Format

calibrate auto-txpower-select disable

undo calibrate auto-txpower-select disable

Parameters

None

Views

RRM profile 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.

Example

# Disable automatic transmit power selection in the RRM profile **802.11b**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name 802.11b
[HUAWEI-wlan-rrm-prof-802.11b] calibrate auto-txpower-select disable
```

11.2.13 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 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* }

undo calibrate enable

Parameters

Parameter	Description	Value
auto	Sets the radio calibration mode to auto.	-
interval *interval-value*	Specifies the radio calibration interval in auto 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 radio calibration in automatic mode.	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.	-
schedule	Sets the radio calibration mode to schedule.	-

Parameter	Description	Value
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.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

There are three radio calibration modes:

- Automatic radio calibration mode: The device periodically implements radio calibration at certain intervals (the interval is specified by **interval** and the default interval is 1440 minutes).
- Manual radio calibration mode: Radio calibration is not automatically implemented by the device but manually triggered through the **11.2.19 calibrate manual startup** command.
- Schedule radio calibration mode: The device triggers radio calibration at the time specified by the parameter **time**.

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 the calibration. In **manual** mode, the device implements radio calibration only after the **calibrate manual startup** command is executed.

Example

# Set the radio calibration mode to manual.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable manual
```

# Set the radio calibration mode to schedule and set the time for scheduled radio calibration to 20:30:00.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable schedule time 20:30:00
```

Related Topics

11.2.19 calibrate manual startup

11.2.14 calibrate error-rate-check

Function

The **calibrate error-rate-check** command configures the interval and traffic threshold for checking the bit error rate (BER).

The **undo calibrate error-rate-check** command configures the interval and traffic threshold for checking the BER.

The default interval and traffic threshold for checking the BER are 1 minute and 1250 kbit/s, respectively.

Format

calibrate error-rate-check interval *interval* **traffic-threshold** *traffic-threshold*

undo calibrate error-rate-check

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for checking the BER.	The value is an integer that ranges from 1 to 10, in minutes.
traffic-threshold *traffic-threshold*	Specifies the traffic threshold for checking the BER.	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 error-rate-check** command to lower the sensitivity for collecting radio BER statistics. When the rate of network traffic reaches the threshold, BER check is performed at the specified interval.

Example

# Set the interval and traffic threshold for checking the BER 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 error-rate-check interval 2 traffic-threshold 1000
```

Related Topics

11.2.15 calibrate error-rate-threshold

11.2.31 display rrm-profile

11.2.15 calibrate error-rate-threshold

Function

The **calibrate error-rate-threshold** command sets the bit error rate (BER) threshold.

The **undo calibrate error-rate-threshold** command restores the default BER threshold.

By default, the BER threshold is 60%.

Format

calibrate error-rate-threshold *error-rate-threshold*

undo calibrate error-rate-threshold

Parameters

Parameter	Description	Value
error-rate-threshold	Specifies the BER 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

If the MAC layer of a radio does not receive any ACK packet after sending a packet at the lowest rate, it considers that an error occurs.

The BER threshold determines whether the radio environment is normal. When the BER 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 BER threshold to 70% in the RRM profile **80211b**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name 80211b
[HUAWEI-wlan-rrm-prof-80211b] calibrate error-rate-threshold 70
```

11.2.16 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
```

Related Topics

11.2.17 calibrate max-tx-power

11.2.18 calibrate min-tx-power

11.2.31 display rrm-profile

11.2.17 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 *power*

undo calibrate max-tx-power

Parameters

Parameter	Description	Value
max-tx-power *power*	Specifies the maximum transmit power that can be adjusted through 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 larger 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 powers using the **calibrate max-tx-power** and **calibrate min-tx-power** commands. The valid power after radio calibration is between the two values. If the values are set improperly, the maximum and minimum calibration power settings may fail to take effect.

- If the maximum calibration power is smaller than the minimum transmit power of an AP, the minimum transmit power takes effect. For example, if the minimum transmit power of an AP on the 2.4 GHz band is 9 dBm and the maximum calibration power is set to 8 dBm, the transmit power on the 2.4 GHz band is 9 dBm after radio calibration.
- If the minimum calibration power is larger than the maximum transmit power of an AP, the maximum transmit power takes effect. For example, if the maximum transmit power on the 2.4 GHz band is 21 dBm and the minimum calibration power is set to 25 dBm, the transmit power on the 2.4 GHz band is 21 dBm after radio calibration.

Example

# Set the maximum transmit power that can be adjusted through 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
```

Related Topics

11.2.18 calibrate min-tx-power

11.2.16 calibrate tpc threshold

11.2.31 display rrm-profile

11.2.18 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 radio calibration is 9 dBm.

Format

calibrate min-tx-power *power*

undo calibrate min-tx-power

Parameters

Parameter	Description	Value
min-tx-power *power*	Specifies the minimum transmit power that can be adjusted through 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 calculates 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 maximum radio calibration power must be larger or equal to the minimum 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 powers using the **calibrate max-tx-power** and **calibrate min-tx-power** commands. The valid power after radio calibration is between the two values. If the values are set improperly, the maximum and minimum calibration power settings may fail to take effect.

- If the maximum calibration power is smaller than the minimum transmit power of an AP, the minimum transmit power takes effect. For example, if the minimum transmit power of an AP on the 2.4 GHz band is 9 dBm and the maximum calibration power is set to 8 dBm, the transmit power on the 2.4 GHz band is 9 dBm after radio calibration.
- If the minimum calibration power is larger than the maximum transmit power of an AP, the maximum transmit power takes effect. For example, if the maximum transmit power on the 2.4 GHz band is 21 dBm and the minimum calibration power is set to 25 dBm, the transmit power on the 2.4 GHz band is 21 dBm after radio calibration.

Example

# Set the minimum transmit power that can be adjusted through 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
```

Related Topics

11.2.17 calibrate max-tx-power

11.2.16 calibrate tpc threshold

11.2.31 display rrm-profile

11.2.19 calibrate manual startup

Function

The **calibrate manual startup** command manually triggers radio calibration.

Format

calibrate manual startup

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

To implement radio calibration instantly, you can run the **calibrate enable** { **auto** [**interval** *interval-value* [**start-time** *start-time*]] | **manual** | **schedule time** *time-value* } command to enable radio calibration and then run the **calibrate manual startup** command to manually trigger radio calibration.

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
```

Related Topics

11.2.13 calibrate enable { auto | manual | schedule time }

11.2.20 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.

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
```

11.2.21 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 { **rogue-ap** | **load** | **non-wifi** | **noise-floor** }

undo calibrate policy { **rogue-ap** | **load** | **non-wifi** | **noise-floor** }

Parameters

Parameter	Description	Value
rogue-ap	Indicates the rogue AP mode.	-
load	Indicates the load mode.	-
non-wifi	Indicates the non-Wi-Fi mode.	-
noise-floor	Indicates the noise floor mode.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Radio calibration policies are classified into:

NOTE

The noise floor, rogue AP and non-Wi-Fi policies take effect only in automatic radio calibration mode.

- Rogue AP policy: When rogue APs (out of control by an AC) exist on a network, set the radio calibration policy to **rogue-ap**. The device then immediately takes actions to avoid interference. This policy may lead to frequency channel switchovers. You are advised to use this policy under the instruction of technical support personnel.
- Load policy: When this radio calibration policy is used, the AP traffic load difference is considered for channel allocation. The device allocates channels with less interference to APs with heavier loads. The AP load changes with times. You are advised to use this policy under the instruction of technical support personnel.
- Non-Wi-Fi policy: When non-Wi-Fi interference occurs on a network, the device immediately takes actions to avoid interference.
- 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.

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

# Set the radio calibration policy to rogue AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate policy rogue-ap
```

11.2.22 calibrate sensitivity

Function

The **calibrate sensitivity** command configures the radio calibration sensitivity for a device.

The **undo calibrate sensitivity** command restores the default radio calibration sensitivity.

By default, the radio calibration sensitivity of the device is set to **medium**.

Format

calibrate sensitivity { **low** | **medium** | **high** }

undo calibrate sensitivity

Parameters

Parameter	Description	Value
low	Indicates low radio calibration sensitivity.	-
medium	Indicates medium radio calibration sensitivity.	-
high	Indicates high radio calibration sensitivity.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Radio calibration sensitivity of a device is described as follows:

- high: Radio calibration is performed when the total interference can be mitigated.
- medium: Radio calibration is performed when the total interference can be mitigated to a large extent.
- low: Radio calibration performed when the total interference can be significantly mitigated.

The default value is recommended.

Example

# Set the radio calibration sensitivity to high.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate sensitivity high
```

11.2.23 calibrate virtual-group-size

Function

The **calibrate virtual-group-size** command sets the channel calibration group size and K value.

The **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
```

11.2.24 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

This command takes effect only on the AD9430DN-12 (including matching RUs), AD9430DN-24 (including matching RUs), AD9431DN-24X (including matching RUs), AP1050DN-S, AP2030DN, AP2050DN, AP2050DN-S, AP2050DN-E, AP3030DN, AP4030DN, AP4130DN, AP4030DN-E, AP4030TN, AP4050DN-E, AP4050DN-HD, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP4051DN-S, AP4051TN, AP430-E, AP5030DN, AP5030DN-S, AP5130DN, AP6050DN, AP6150DN, AP6052DN, AP7050DN-E, AP7050DE, AP7052DN, AP7152DN, AP7052DE, AP8030DN, AP8130DN, AP8130DN-W, AP8050DN, AP8150DN, AP8050DN-S, AP8050TN-HD, AP8082DN, AP8182DN, AP9131DN, AP9132DN, and AP9330DN.

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

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 a WLAN chip to determine whether the channel is idle. If the noise on the channel exceeds the threshold, the chip considers the channel busy. Otherwise, the chip considers the channel idle.

When deploying a WLAN, set a proper CCA threshold to reduce signal interference and improve the channel reuse rate.

- If APs are densely deployed, a high CCA threshold is recommended to narrow down the coverage and skip remote weak signals.
- If APs are sparsely deployed, a low CCA threshold is recommended to maximize the effective coverage of signals.

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 may affect uplink access coverage or STA access. Modify this parameter only
under the guidance of technical
personnel. Continue? [Y/N]Y
```

11.2.25 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 is 20 MHz.

Format

dca-channel 5g bandwidth { **20mhz** | **40mhz** | **80mhz** }

undo dca-channel 5g bandwidth

Parameters

Parameter	Description	Value
5g	Specifies the frequency band on which radio calibration is implemented.	-
20mhz | **40mhz** | **80mhz**	Specifies the calibration bandwidth.	-

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 5 GHz frequency band has richer spectrum resources. In addition to 20 MHz channels, APs working on the 5 GHz frequency band support 40 MHz and 80 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 **11.2.26 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

Only the AP2030DN, AP1050DN-S, AP8050DN, AP8050DN-S, AP8150DN, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP2050DN, AP2050DN-E, AP4030DN, AP4130DN, AP5030DN, AP4030TN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DN-E, AP5130DN, AP7030DE, AP9131DN, AP9132DN, AD9430DN-24 central AP (including the mapping RUs), AD9430DN-12 central AP (including the mapping RUs), AD9431DN-24X central AP (including the mapping RUs), AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP9330DN, AP8030DN, AP8130DN-W, and AP8130DN support 80 MHz calibration bandwidth.

When configuring 40 MHz or 80 MHz calibration bandwidth, check whether channels of the corresponding bandwidth exist under the country code.

Example

# Set the calibration bandwidth to 40 MHz.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name huawei
[HUAWEI-wlan-regulate-domain-huawei] dca-channel 5g bandwidth 40mhz
```

Related Topics

11.2.26 dca-channel channel-set

11.1.141 display regulatory-domain-profile

11.2.26 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 the 2.4G radio and contains all channels supported by the corresponding country code on the 5G radio. If the country code is China, the calibration channel set does not contain channels 36 to 64. When configuring the calibration channels, users can specify channels as prompted.

Format

dca-channel { **2.4g** | **5g** } **channel-set** *channel-value*

undo dca-channel { **2.4g** | **5g** } **channel-set**

Parameters

Parameter	Description	Value
2.4g | **5g**	Specifies the frequency band on which radio calibration is performed. ● **2.4g**: Radios work on the 2.4 GHz frequency band. ● **5g**: Radios work on the 5 GHz frequency band.	-
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

The 5 GHz frequency band has richer spectrum resources. In addition to 20 MHz channels, APs working on the 5 GHz frequency band support 40 MHz and 80 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 **11.2.25 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 channels you configure must be supported by the terminals; otherwise, the terminals cannot discover wireless 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.

For three 5G radios, configure at least five calibration channels. For two 5G 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 huawei
[HUAWEI-wlan-regulate-domain-huawei] dca-channel 5g bandwidth 40mhz
[HUAWEI-wlan-regulate-domain-huawei] dca-channel 5g channel-set 149,153,157,161
```

Related Topics

11.1.77 country-code

11.2.25 dca-channel bandwidth

11.2.27 deny-threshold

Function

The **deny-threshold** command configures the maximum number of times an AP rejects association requests of a STA for a static load balancing group.

The **undo deny-threshold** command restores the default maximum number of times an AP rejects association requests of a STA for a static load balancing group.

By default, the maximum number of times an AP rejects association requests of a STA is 3 for a static load balancing group.

Format

deny-threshold *deny-threshold*

undo 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 1 to 10.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

You can run the **deny-threshold** command to set the maximum number of times an AP rejects association requests of a STA for a static load balancing group. When a STA requests to associate with an AP radio in the static load balancing group, the AP rejects the association request of the STA if traffic is not balanced among radios in the group. When the number of consecutive association attempts of the STA exceeds the configured maximum number of rejection times, the AP allows the STA to associate with it regardless of whether traffic is balanced.

Example

# Set the maximum number of times an AP rejects association requests of a STA to 8 for 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] deny-threshold 8
```

Related Topics

11.2.85 sta-load-balance static-group

11.2.28 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
huawei               1
------------------------------------------------------------
Total: 2
```

Table 11-103 Description of the **display air-scan-profile all** command output

Item	Description
Profile name	Name of an air scan profile.
Reference	Number of times that the air scan profile is referenced.

# Display information about the air scan profile **huawei**.

```
<HUAWEI> display air-scan-profile name huawei
-----------------------------------------------------------
Scan switch       : enable
Scan period(ms)   : 80
Scan interval(ms) : 3000
Scan channel-set  : dca-channel
-----------------------------------------------------------
```

Table 11-104 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 **11.2.56 scan-disable** command.
Scan period(ms)	Air scan period. To set the air scan period, run the **11.2.58 scan-period** command.
Scan interval(ms)	Air scan interval. To set the air scan interval, run the **11.2.57 scan-interval** command.
Scan channel-set	Air scan channel set. To set the air scan channel set, run the **11.2.55 scan-channel-set** command.

Related Topics

11.2.56 scan-disable

11.2.58 scan-period

11.2.57 scan-interval

11.2.55 scan-channel-set

11.2.29 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 **huawei**.

```
<HUAWEI> display references air-scan-profile name huawei
------------------------------------------------------------
Reference type                 Reference name
------------------------------------------------------------
radio-2g-profile               default
------------------------------------------------------------
Total: 1
```

Table 11-105 Description of the display references air-scan-profile command output

Item	Description
Reference type	Type of the profile that references the air scan profile.

Item	Description
Reference name	Name of the profile that references the air scan profile.

11.2.30 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 **huawei**.

```
<HUAWEI> display references rrm-profile name huawei
------------------------------------------------------------
Reference type           Reference name
------------------------------------------------------------
radio-2g-profile         radio0
radio-5g-profile         radio1
------------------------------------------------------------
Total: 2
```

Table 11-106 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.

11.2.31 display rrm-profile

Function

The **display rrm-profile** command displays information about an RRM profile.

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 this command to view information about an RRM profile.

Example

# Display information about all RRM profiles.

```
<HUAWEI> display rrm-profile all
------------------------------------------------------------
Profile name  Reference
------------------------------------------------------------
default       2
```

```
------------------------------------------------------------
Total:1
```

Table 11-107 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 **huawei**.

```
<HUAWEI> display rrm-profile name huawei
----------------------------------------------------------------------------
Auto channel select                                            : enable
Auto transmit power select                                     : enable
PER threshold for trigger channel/power select(%)              : 60
Noise-floor threshold for trigger channel/power select(dBm)  : -60
Calibrate tpc threshold(dBm):                                  : -60
Calibrate maximum TX power(dBm):                               : 127
Calibrate minimum TX power(dBm):                               : 1
Calibrate error rate check interval(min)                       : 1
Calibrate error rate check traffic threshold(kbps)             : 1250
Airtime fairness schedule                                      : disable
Dynamic adjust EDCA parameter                                  : enable
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
UAC check channel utilization                                  : disable
UAC channel utilization access threshold(%)                    : 80
UAC channel utilization roam threshold(%)                      : 80
UAC hide SSID                                                  : disable
Band steer deny threshold                                      : 5
Band steer SNR threshold(dB)                                   : 20
Band balance start threshold                                   : 10
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 deny threshold                            : 6
Station load balance RSSI threshold(dBm)                       : -70
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 channel-utilization start threshold(%)   : 50
Station load balance channel-utilization gap threshold(%)     : 20
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
Smart-roam                                                     : 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
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
----------------------------------------------------------------------
```

Table 11-108 Description of the **display rrm-profile name** command output

Item	Description
Auto channel select	Whether to enable automatic channel selection. To configure this parameter, run the **11.2.11 calibrate auto-channel-select disable** command.
Auto transmit power select	Whether to enable automatic transmit power selection. To configure this parameter, run the **11.2.12 calibrate auto-txpower-select disable** command.
PER threshold for trigger channel/ power select(%)	PER threshold for triggering channel or power adjustment. To configure this parameter, run the **11.2.15 calibrate error-rate-threshold** command.
Noise-floor threshold for trigger channel/power select(dBm)	Noise-floor threshold for triggering channel or power adjustment. To configure this parameter, run the **11.2.20 calibrate noise-floor-threshold** command.
Calibrate tpc threshold(dBm)	TPC coverage threshold. To configure this parameter, run the **11.2.16 calibrate tpc threshold** command.

Item	Description
Calibrate maximum TX power(dBm)	Maximum transmit power that can be adjusted through radio calibration. To configure this parameter, run the **11.2.17 calibrate max-tx-power** command.
Calibrate minimum TX power(dBm)	Minimum transmit power that can be adjusted through radio calibration. To configure this parameter, run the **11.2.18 calibrate min-tx-power** command.
Calibrate error rate check interval(min)	Interval for checking the BER. To configure this parameter, run the **11.2.14 calibrate error-rate-check** command.
Calibrate error rate check traffic threshold(kbps)	Traffic threshold for checking the BER. To configure this parameter, run the **11.2.14 calibrate error-rate-check** command.
Airtime fairness schedule	Whether to enable airtime fair scheduling. To configure this parameter, run the **11.5.2 airtime-fair-schedule enable** command.
Dynamic adjust EDCA parameter	Whether to enable dynamic EDCA parameter adjustment. To configure this parameter, run the **11.2.40 dynamic-edca enable** command.
UAC check client's SNR	Whether to enable user CAC based on terminal SNR. To configure this parameter, run the **11.2.95 uac enable** command.
UAC client's SNR threshold(dB)	User CAC SNR threshold. To configure this parameter, run the **11.2.98 uac client-snr threshold** command.
UAC check client number	Whether to enable user CAC based on the number of users. To configure this parameter, run the **11.2.95 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 **11.2.96 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 **11.2.96 uac client-number threshold** command.
UAC check channel utilization	Whether to enable user CAC based on the channel usage. To configure this parameter, run the **11.2.95 uac enable** command.
UAC channel utilization access threshold(%)	User CAC access threshold based on the channel usage. To configure this parameter, run the **11.2.94 uac channel-utilization threshold** command.
UAC channel utilization roam threshold(%)	User CAC roaming threshold based on the channel usage. To configure this parameter, run the **11.2.94 uac channel-utilization threshold** command.
UAC hide SSID	Whether to enable SSID hiding for User CAC. To configure this parameter, run the **11.2.99 uac reach-access-threshold hide-ssid** 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 **11.2.8 band-steer deny-threshold** command.
Band steer SNR threshold(dB)	Start SNR threshold for triggering 5G-prior access. To configure this parameter, run the **11.2.10 band-steer snr-threshold** command.

Item	Description
Band balance start threshold	Start threshold for load balancing between radios. To configure this parameter, run the **11.2.6 band-steer balance start-threshold** command.
Band balance gap threshold(%)	Load difference threshold for load balancing between radios. To configure this parameter, run the **11.2.5 band-steer balance gap-threshold** command.
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 **11.2.7 band-steer client-band-expire** command.
Station load balance	Whether to enable the load balancing function. To configure this parameter, run the **11.2.79 sta-load-balance dynamic enable** command.
Station load balance mode	Dynamic load balancing mode. ● channel-utilization: dynamic load balancing based on the channel usage ● sta-number: dynamic load balancing based on the number of users. To configure this parameter, run the **11.2.90 sta-load-balance mode** command.
Station load balance deny threshold	Maximum number of times an AP rejects association requests of a STA for dynamic load balancing. To configure this parameter, run the **11.2.78 sta-load-balance dynamic deny-threshold** command.

Item	Description
Station load balance RSSI threshold(dBm)	RSSI threshold for member devices in a dynamic load balancing group. To configure this parameter, run the **11.2.89 sta-load-balance dynamic rssi-threshold** 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 **11.2.81 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 **11.2.80 sta-load-balance dynamic sta-number gap-threshold** command.
Station load balance sta-number gap threshold(number)	Load difference threshold for static load balancing based on the number of users. To configure this parameter, run the **11.2.80 sta-load-balance dynamic sta-number gap-threshold** command.
Station load balance channel-utilization start threshold(%)	Start threshold for dynamic load balancing based on the channel usage. To configure this parameter, run the **11.2.88 sta-load-balance dynamic channel-utilization start-threshold** command.
Station load balance channel-utilization gap threshold(%)	Load difference threshold for dynamic load balancing based on the channel usage. To configure this parameter, run the **11.2.87 sta-load-balance dynamic channel-utilization gap-threshold** command.
Station load balance deauth fail times	Maximum number of attempts to migrate STAs in deauthentication mode. To configure this parameter, run the **11.2.77 sta-load-balance dynamic deauth-fail-times** command.

Item	Description
Station load balance BTM fail times	Maximum number of attempts to migrate STAs in BTM mode. To configure this parameter, run the **11.2.76 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 migration of the STAs. To configure this parameter, run the **11.2.84 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 migration of the STAs. To configure this parameter, run the **11.2.83 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 migration of the STAs. To configure this parameter, run the **11.2.82 sta-load-balance dynamic steer-restrict auth-threshold** command.
Smart-roam	Whether to enable smart roaming. To configure this parameter, run the **11.2.65 smart-roam disable** command.
Smart-roam quick kickoff	Whether to enable the function of quickly disconnecting STAs. To configure this parameter, run the **11.2.67 smart-roam quick-kickoff-threshold disable** command.
Smart-roam check SNR	Whether to specify the trigger mode of smart roaming as **check SNR**. To configure this parameter, run the **11.2.72 smart-roam roam-threshold { check-snr | check-rate }** command.

Item	Description
Smart-roam quick kickoff check SNR	Whether to enable the function of quickly disconnecting STAs is triggered by checking the SNR of STAs. To configure this parameter, run the **11.2.68 smart-roam quick-kickoff-threshold { check-snr | check-rate }** command.
Smart-roam check rate	Whether to specify the trigger mode of smart roaming as **check rate**. To configure this parameter, run the **11.2.72 smart-roam roam-threshold { check-snr | check-rate }** command.
Smart-roam quick kickoff check rate	Whether to enable the function of quickly disconnecting STAs is triggered by checking the rate of STAs. To configure this parameter, run the **11.2.68 smart-roam quick-kickoff-threshold { check-snr | check-rate }** command.
Smart-roam standing SNR threshold(dB)	SNR threshold for smart roaming. To configure this parameter, run the **11.2.73 smart-roam roam-threshold { snr | rate }** command.
Smart-roam SNR quick-kickoff-threshold(dB)	SNR-based 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 **11.2.73 smart-roam roam-threshold { snr | rate }** command.
Smart-roam rate quick-kickoff-threshold(%)	Rate-based 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 terminal roaming. To configure this parameter, run the **11.2.74 smart-roam snr-margin** command.

Item	Description
Smart-roam low level SNR margin(dB)	Lower SNR difference threshold that triggers terminal roaming. To configure this parameter, run the **11.2.74 smart-roam snr-margin** command.
Smart-roam SNR check interval(s)	Terminal SNR check interval. To configure this parameter, run the **11.2.69 smart-roam quick-kickoff-snr check-interval** command.
Smart-roam unable roam client expire time(min)	Aging time of "unable to roam" record. To configure this parameter, run the **11.2.75 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 **11.2.69 smart-roam quick-kickoff-snr check-interval** command.
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 **11.2.70 smart-roam quick-kickoff-snr p-n criteria** command.
Smart-roam quick-kickoff SNR P-N qualify time	Number of times criteria are met to determine whether to quickly disconnect STAs. To configure this parameter, run the **11.2.70 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 **11.2.64 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 **11.2.66 smart-roam quick-kickoff back-off-time** command.

Item	Description
AMC policy	Adaptive modulation and coding (AMC) algorithm. To configure this parameter, run the **11.2.2 amc-policy** command.
High density AMC optimize	Whether to enable the AMC optimization function in high-density scenarios. To configure this parameter, run the **11.2.44 high-density amc-optimize enable** command.
SFN roam check high threshold(dBm)	Upper RSSI threshold for agile distributed SFN roaming. To configure this parameter, run the **11.4.13 sfn-roam roam-check high-threshold** command.
SFN roam check low threshold(dBm)	Lower RSSI threshold for agile distributed SFN roaming. To configure this parameter, run the **11.4.14 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 **11.4.11 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 **11.4.9 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 **11.4.15 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 **11.4.16 sfn-roam roam-check sta-holding times** command.

Item	Description
SFN roam check gap-rssi(dB)	RSSI gap for agile distributed SFN roaming RUs. To configure this parameter, run the **11.4.12 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 **11.4.10 sfn-roam roam-check better-times** command.
DFS smart select	Whether to enable DFS smart selection. ● enable: DFS smart selection is enabled. ● disable: DFS smart selection is disabled. To configure this parameter, run the **11.2.42 dfs smart-selection disable** command.
DFS recover delay time(min)	Delay in switching back the DFS channel. To configure this parameter, run the **11.2.41 dfs recover-delay** command.

11.2.32 display sta-load-balance static-group

Function

The **display sta-load-balance static-group** command displays information about a static load balancing group.

Format

display sta-load-balance static-group { **all** | **name** *group-name* }

Parameters

Parameter	Description	Value
all	Displays information about all static load balancing groups.	-

Parameter	Description	Value
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 group.

```
<HUAWEI> display sta-load-balance static-group all
------------------------------------------------------------
Index  Group name
------------------------------------------------------------
0      cc
1      coco
------------------------------------------------------------
Total: 2
```

Table 11-109 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 status                 : balance
Load-balance mode                   : channel-utilization
Deny threshold                      : 8
Sta-number start threshold          : 40
Sta-number gap threshold(percentage)   : 20
Sta-number gap threshold(number)       : -
Channel-utilization start threshold(%) : 50
Channel-utilization gap threshold(%)   : 20
-------------------------------------------------------------------
```

```
RfID: Radio ID
CurEIRP: Current EIRP (dBm)
Act CH: Actual channel, Cfg CH: Config channel, CU: Channel utilization
-----------------------------------------------------------------
AP ID  AP Name  RfID  Act CH/Cfg CH  CurEIRP/MaxEIRP  Client  CU
-----------------------------------------------------------------
2      area_2   0     6/-            28/28            0       37%
2      area_2   1     153/-            29/29            0       76%
3      area_3   0     1/-            28/28            0       68%
3      area_3   1     149/-            29/29            0       5%
-----------------------------------------------------------------
Total: 4
```

Table 11-110 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 status	Load balancing status in a static load balancing group.
Load-balance mode	Load balancing mode. • channel-utilization: dynamic load balancing based on the channel usage • sta-number: dynamic load balancing based on the number of users. To configure this parameter, run the **11.2.92 mode (static load balancing group view)** command.
Deny threshold	Maximum number of times an AP rejects association requests of a STA in a static load balancing group. To configure this parameter, run the **11.2.27 deny-threshold** command.
Sta-number start threshold	Start threshold for load balancing based on the number of users in a static load balancing group. To configure this parameter, run the **11.2.86 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 **11.2.43 sta-number gap-threshold** command.

Item	Description
Sta-number gap threshold(number)	Load difference threshold for static load balancing based on the number of users. To configure this parameter, run the **11.2.43 sta-number gap-threshold** command.
Channel-utilization start threshold(%)	Start threshold for load balancing based on the channel usage in a static load balancing group. To configure this parameter, run the **11.2.93 channel-utilization start-threshold** command.
Channel-utilization gap threshold(%):	Load difference threshold for load balancing based on the channel usage in a static load balancing group. To configure this parameter, run the **11.2.91 channel-utilization gap-threshold** command.
AP ID	ID of the AP that joins a static load balancing group.
AP Name	Name of the AP that joins a static load balancing group.
RfID	Radio that joins a static load balancing group.
Act CH/Cfg CH	Actual effective/configured channel of an AP.
CurEIRP/MaxEIRP	Current power of an AP radio/ Maximum power of an AP radio.
Client	Number of STAs connected to an AP radio.
CU	Usage of a channel.

Related Topics

11.2.86 sta-number start-threshold

11.2.43 sta-number gap-threshold

11.2.27 deny-threshold

11.2.33 display station load-balance sta-mac

Function

The **display station load-balance sta-mac** command displays information about the dynamic load balancing group based on STAs.

Format

display station load-balance sta-mac *mac-address*

Parameters

Parameter	Description	Value
mac-address	Displays information about the dynamic load balancing group based on the STA with the specified MAC address.	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

After dynamic load balancing group configuration is complete, run the **display station load-balance sta-mac** command to check information about the group based on STAs.

Example

# Display information about the dynamic load balancing group.

```
<HUAWEI> display station load-balance sta-mac a826-d9e5-6df3
Station load balance status: Balance
---------------------------------------------------------------------------
AP name                          Radio ID        AP MAC
---------------------------------------------------------------------------
ap1                            0             00da-a8c1-e400
ap3                            0             dcd2-fc96-e4c0
---------------------------------------------------------------------------
Total: 2
```

Table 11-111 Description of the **display station load-balance sta-mac** command output

Item	Description
Station load balance status	Load balancing status in the dynamic load balancing group: ● Balance: the load is balanced. ● Not balance: the load is unbalanced.
AP name	Name of the AP in the load balancing group.
Radio ID	ID of the radio in the load balancing group.
AP MAC	MAC address of the AP in the load balancing group.

11.2.34 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 d022-be5e-021f
--------------------------------------------------------------------------------
----------------------------------------
 AP MAC           AP ID    AP Name           Radio ID       Probe info(RSSI/HH
:MM:SS)   11k info[RCPI/RSNI/HH:MM:SS]
--------------------------------------------------------------------------------
----------------------------------------
 1047-80ab-c9a0    5        AP5               1             -48/16:28:24
        205/45/16:28:24
--------------------------------------------------------------------------------
----------------------------------------
```

System Response

Table 11-112 Description of the **display station neighbor** command output

Item	Description
AP MAC	MAC address of a neighboring AP.
AP ID	ID of a neighboring AP.
AP Name	Name of a neighboring AP.
Radio ID	Radio ID of a neighboring AP.
Probe info(RSSI/ HH :MM:SS)	Probe information about the STA, including the RSSI and timestamp.
11k info[RCPI/RSNI/ HH:MM:SS]	802.11k information about the STA, including the Received Channel Power Indicator, Received Signal-to-Noise Indication, and timestamp. **NOTE** If the STA does not support 802.11k, this parameter is displayed as "-".

11.2.35 display station steer-history

Function

The **display station steer-history** command displays historical information about STA migrations.

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 migrated. You can run this command to check historical information about STA migrations.

Example

# Display historical information about migrations of all STAs.

```
<HUAWEI> display station steer-history
TO:Time Out
S/T/A:Source/Target/Actual
Flag:V[Voice/Video/Active STA]
--------------------------------------------------------------------------------
----------------------------------------------------
Time                 Sta           AP(S/T/A)      Radio(S/T/A)   Rssi(S/T/A)
Reason       Move-mode  BTM_CODE  Flag      Result
--------------------------------------------------------------------------------
----------------------------------------------------
2018-03-28/23:07:34   b0e2-35c3-d09c 6/3/3         1/1/0         0/-/-
LoadBalance  BTM        0         100       Success
2018-03-28/23:07:34   b0e2-35c3-d09d 6/3/6         1/1/0         0/-/-
LoadBalance  BTM        1         -         Failed
--------------------------------------------------------------------------------
----------------------------------------------------
Total: 2
```

Table 11-113 Description of the **display station steer-history** command output

Item	Description
Time	Time when a STA is triggered to migrate.
Sta	MAC address of a STA.
AP(S/T/A)	ID of the source AP/ID of the destination AP/ID of the AP to which a STA actually migrates.
Radio(S/T/A)	ID of the source radio/ID of the destination radio/ID of the radio to which a STA actually migrates.
Rssi(S/T/A)	RSSI of the source radio/RSSI of the destination radio/RSSI of the radio to which a STA actually migrates.
Reason	Reason why a STA is triggered to migrate.

Item	Description
Move-mode	Migration mode of a STA.
BTM_CODE	BTM migration 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 migrates in deauthentication mode or the device does not receive any BTM response.
Flag	Voice STA flag/Video STA flag/Active STA flag.
Result	Migration result of a STA.

11.2.36 display station steer-statistics

Function

The **display station steer-statistics** command displays statistics about STA migrations.

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 migrated. You can run this command to check statistics about STA migrations.

Example

# Display statistics about migrations of all STAs.

```
<HUAWEI> display station steer-statistics
--------------------------------------------------------------------------------
------------------------------------------------
Reason          Total/Success   Deauth(Total/Success)  BTM(Total/Accept/REJ1/ RE
J2/ REJ3/ REJ4/ REJ5/ REJ6/ REJ7/ REJ8/ TimeOut)
--------------------------------------------------------------------------------
------------------------------------------------
Sticky                0/0             0/0             0/0/0/0/0/0/0/0/0/0/0
Load-balance             0/0             0/0             0/0/0/0/0/0/0/0/0/0/0
Band-steer              0/0             0/0             0/0/0/0/0/0/0/0/0/0/0
Total                 0/0             0/0             0/0/0/0/0/0/0/0/0/0/0
--------------------------------------------------------------------------------
------------------------------------------------
```

Table 11-114 Description of the **display station steer-statistics** command output

Item	Description
Reason	Reason why a STA is triggered to migrate. ● Sticky: The STA is sticky. ● Load-balance: Load balancing is implemented. ● Band-steer: Band steering is implemented.
Total/Success	Total number of triggered STA migrations/Number of successful STA migrations.
Deauth(Total/Success)	Total number of STA migrations triggered in deauthentication mode/ Number of successful STA migrations triggered in deauthentication mode.

Item	Description
BTM(Total/Accept/REJ1/ REJ2/ REJ3/ REJ4/ REJ5/ REJ6/ REJ7/ REJ8/ TimeOut)	Total number of STA migrations triggered in BTM mode/Number of successful STA migrations triggered in BTM mode/Number of rejected STA migrations in BTM mode/Number of STA migrations that are 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.

11.2.37 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
------------------------------------------------------------------------------
FCFC-4895-C87E      3h 20m
581F-28FC-7EAD      2h 30m
------------------------------------------------------------------------------
Total: 2
```

Table 11-115 Description of the **display station unsteerable** command output

Parameter	Description
STA MAC	MAC address of the "unable to roam" STA.
Left aging time	Remaining aging period.

11.2.38 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
-------------------------------------------------------------------------------

AP group     : mainland
Country code: CN
-------------------------------------------------------------------------------
Radio band  Bandwidth  Channel Set
-------------------------------------------------------------------------------
2.4G        20MHz      1,6,11
5G          20MHz      149,153,157,161,165
-------------------------------------------------------------------------------
```

Table 11-116 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.

Related Topics

11.2.25 dca-channel bandwidth

11.2.26 dca-channel channel-set

11.2.39 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 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 identify a radio.	The AP ID must already exist.
radio *radio-id*	Displays radio calibration statistics on the specified radio.	The value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

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 of AP **office**.

```
<HUAWEI> display wlan calibrate statistics ap-name office radio 0
------------------------------------------------------------------------
Signal environment deterioration :1
```

```
Power calibration              :1
Channel calibration             :0
----------------------------------------------------------------------
```

Table 11-117 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.

Related Topics

11.2.52 reset wlan calibrate statistics

11.2.40 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 huawei
[HUAWEI-wlan-rrm-prof-huawei] dynamic-edca enable
```

Related Topics

11.2.31 display rrm-profile

11.2.41 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

When an AP is working on the manually planned channel, if radar signals are detected, the AP randomly selects a channel (the calibration channel preferentially) allowed by the country code. 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
```

Related Topics

11.2.31 display rrm-profile

11.2.42 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 randomly selects a channel allowed by the country code to prevent radar interference.

The switched-to channel is a random non-radar channel and therefore may be the same as or close to the channel of surrounding 5 GHz radios, leading to severe interference and poor user experience. The DFS smart selection function is enabled by default to adjust the 5 GHz channel of an AP to one with the least 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.
```

Related Topics

11.2.31 display rrm-profile

11.2.43 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 based on the percentage of users is 20%.

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

After the load difference threshold for load balancing based on the number of users is configured using the **sta-number gap-threshold** command, an AP implements load balancing based on the difference between the number of users on different radios. The load balancing algorithm is as follows:

Load balancing algorithm based on the percentage of users: The AC calculates the load percentage of each radio in a load balancing group using the formula: Load percentage of a radio = (Number of associated users on the radio/Maximum number of users allowed on the radio) x 100%. The AC compares load percentages of all radios in the load balancing group and obtains the smallest load percentage value. When a user requests to associate with an AP radio, the AC calculates the difference between the radio's load percentage and the smallest load percentage value and compares the load difference with the threshold. If the difference is smaller than the threshold, the AC allows the user to associate with the radio. If not, the AC rejects the association request of the user. If users continue to send association requests to the AP and the maximum number of times the AP rejects users' association requests that is configured using the **11.2.27 deny-threshold** command for a static load balancing group, the AP allows user access.

The load balancing algorithm based on the actual number of users is similar to that based on the percentage of users. The only difference is that the former algorithm uses the number of users actually associated with radios to calculate the difference.

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
```

Related Topics

11.2.85 sta-load-balance static-group

11.2.27 deny-threshold

11.2.44 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

- This takes effect only on APs in compliance with 802.11ac Wave 2.
- 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
```

11.2.45 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 **11.2.47 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.2.47 interference detect-enable

11.2.46 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 **11.2.47 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.2.47 interference detect-enable

11.2.47 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
```

11.2.48 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 **11.2.47 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.2.47 interference detect-enable

11.2.49 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*] }&<1-8>

undo member { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }&<1-8>

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 value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

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 composed of the central AP and RUs, you only need to add radios of the RUs to a static load balancing group.
- 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
```

Related Topics

11.2.85 sta-load-balance static-group

11.2.50 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.

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 mode using the **undo calibrate auto-txpower-select disable** command.

Example

# Enable signal-strength-based power adjustment for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name huawei
[HUAWEI-wlan-radio-2g-prof-huawei] power auto-adjust enable
```

Related Topics

11.2.12 calibrate auto-txpower-select disable

11.2.51 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.
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 value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

Views

WLAN view

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 AP 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] reset ap traffic statistics wireless ap-id 0 radio 2
```

11.2.52 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 identify a radio.	The AP name must already exist.
ap-id *ap-id*	Clears radio calibration statistics on the AP with the specified AP ID. The AP ID and radio ID identify a radio.	The AP ID must already exist.
radio *radio-id*	Clears calibration statistics about the radio with the specified radio ID. The radio ID and AP name identify a radio.	The value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

Views

User view

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 of AP **office**.

```
<HUAWEI> reset wlan calibrate statistics ap-name office radio 0
```

Related Topics

11.2.39 display wlan calibrate statistics

11.2.53 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 **11.2.54 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]
```

Related Topics

11.2.54 rrm-profile (radio profile view)

11.2.54 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 **11.2.53 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
```

Related Topics

11.2.53 rrm-profile (WLAN view)

11.2.55 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 **11.2.26 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, terminal 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 huawei
[HUAWEI-wlan-air-scan-prof-huawei] scan-channel-set dca-channel
```

Related Topics

11.2.28 display air-scan-profile

11.2.56 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, and smart roaming.

Example

# Disable the air scan function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name huawei
[HUAWEI-wlan-air-scan-prof-huawei] 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
```

Related Topics

11.2.28 display air-scan-profile

11.2.57 scan-interval

Function

The **scan-interval** command sets an air scan interval.

The **undo scan-interval** command restores the default air scan profile.

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 2s 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.

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 huawei
[HUAWEI-wlan-air-scan-prof-huawei] scan-interval 3000
```

Related Topics

11.2.28 display air-scan-profile

11.2.58 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.

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 huawei
[HUAWEI-wlan-air-scan-prof-huawei] scan-period 80
```

Related Topics

11.2.28 display air-scan-profile

11.2.59 smart-antenna { enable | disable }

Function

The **smart-antenna** { **enable** | **disable** } command enables or disables the smart antenna function for an AP.

The **undo smart-antenna** command restores the smart antenna function of an AP to the default state.

By default, the smart antenna function is disabled for APs but enabled for the AP7052DE.

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

After the smart antenna function is enabled, an AP can select a proper antenna array based on STAs' locations, improving signal strength and user experience.

Precautions

- The AP7030DE, AP7052DE and AP7050DE support the smart antenna function.

Example

# Enable the smart antenna function 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.2.60 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.2.61 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.
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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.2.62 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.2.63 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
```

Related Topics

11.1.130 display radio-2g-profile

11.1.131 display radio-5g-profile

11.2.64 smart-roam advanced-scan disable

Function

The **smart-roam advanced-scan disable** command disables the coordinated scanning function of smart roaming.

The **undo smart-roam advanced-scan disable** command enables the coordinated scanning function of smart roaming.

By default, the coordinated scanning function of smart 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 the coordinated scanning function of smart 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 the coordinated scanning function of smart roaming 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

Smart roaming has been enabled using the **undo 11.2.65 smart-roam disable** command.

Example

# Enable the coordinated scanning function of smart roaming.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam disable
[HUAWEI-wlan-rrm-prof-default] undo smart-roam advanced-scan disable
```

Related Topics

11.2.65 smart-roam disable

11.2.65 smart-roam disable

Function

The **smart-roam disable** command disables smart roaming.

The **undo smart-roam disable** command enables smart roaming.

By default, smart roaming is enabled.

Format

smart-roam disable

undo smart-roam disable

Parameters

None

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 reinitiating a connection with the AP or roaming to another AP. This degrades user experience. To prevent this situation, configure the smart roaming function. When detecting that the SNR or access rate of a STA is lower than the specified threshold, the AP sends a Disassociation packet to the STA so that the STA can reconnect or roam to another AP.

Follow-up Procedure

Run the **11.2.72 smart-roam roam-threshold { check-snr | check-rate }** command to configure the trigger mode of smart roaming and the **11.2.73 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 huawei
[HUAWEI-wlan-rrm-prof-huawei] undo smart-roam disable
```

Related Topics

11.2.72 smart-roam roam-threshold { check-snr | check-rate }

11.2.73 smart-roam roam-threshold { snr | rate }

11.2.66 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
```

11.2.67 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 using the **undo smart-roam quick-kickoff-threshold disable** command, and the threshold for quickly disconnecting STAs is specified, the AP disconnects STAs whose SNR or access rate is lower the specified threshold. The STAs then can connect to or roam to another AP with stronger signals.

Follow-up Procedure

Run the **11.2.68 smart-roam quick-kickoff-threshold { check-snr | check-rate }** command to set the mode for triggering the function of quickly disconnecting STAs, and the **11.2.71 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
```

Related Topics

11.2.68 smart-roam quick-kickoff-threshold { check-snr | check-rate }

11.2.71 smart-roam quick-kickoff-threshold

11.2.68 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** **11.2.67 smart-roam quick-kickoff-threshold disable** command.

Follow-up Procedure

Run the **11.2.71 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
```

Related Topics

11.2.67 smart-roam quick-kickoff-threshold disable

11.2.71 smart-roam quick-kickoff-threshold

11.2.69 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 11.2.67 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
```

Related Topics

11.2.67 smart-roam quick-kickoff-threshold disable

11.2.70 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.
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 11.2.67 smart-roam quick-kickoff-threshold disable** command.

Precautions

The value of **observe-value** must be larger 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
```

Related Topics

11.2.67 smart-roam quick-kickoff-threshold disable

11.2.69 smart-roam quick-kickoff-snr check-interval

11.2.71 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 75, in 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' SNR or rate from data packets sent from the STA. If the STA' 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 11.2.67 smart-roam quick-kickoff-threshold disable** command.

The mode for triggering the function of quickly disconnecting STAs has been set using the **11.2.68 smart-roam quick-kickoff-threshold { check-snr | check-rate }** command

Example

# Set the mode for triggering the function of quickly disconnecting STAs to **check-rate** and the threshold for quickly disconnecting STAs to 50%.

```
<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
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold rate 50
```

Related Topics

11.2.67 smart-roam quick-kickoff-threshold disable

11.2.68 smart-roam quick-kickoff-threshold { check-snr | check-rate }

11.2.72 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, the smart roaming condition is met. When the smart roaming is triggered, 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

The smart roaming function has been enabled using the **undo** **11.2.65 smart-roam disable** command.

Follow-up Procedure

Run the **11.2.73 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 huawei
[HUAWEI-wlan-rrm-prof-huawei] undo smart-roam disable
[HUAWEI-wlan-rrm-prof-huawei] smart-roam roam-threshold check-rate
```

Related Topics

11.2.65 smart-roam disable

11.2.73 smart-roam roam-threshold { snr | rate }

11.2.73 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, an STA's SNR is lower than the threshold when the STA's RSSI is lower than -70 dBm (25 dB + (-95 dBm) = -70 dBm).	The value is an integer that ranges from 5 to 75, in dB.
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, the smart roaming condition is met. When the smart roaming is triggered, 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

The smart roaming function has been enabled using the **undo** **11.2.65 smart-roam disable** command.

The trigger mode of smart roaming has been configured using the **11.2.72 smart-roam roam-threshold { check-snr | check-rate }** command.

Example

# Set the trigger mode of smart roaming to **check-rate** and set the smart roaming threshold to 50%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] undo smart-roam disable
[HUAWEI-wlan-rrm-prof-huawei] smart-roam roam-threshold check-rate
[HUAWEI-wlan-rrm-prof-huawei] smart-roam roam-threshold rate 50
```

Related Topics

11.2.65 smart-roam disable

11.2.73 smart-roam roam-threshold { snr | rate }

11.2.74 smart-roam snr-margin

Function

The **smart-roam snr-margin** command sets the SNR difference threshold that triggers terminal roaming.

The **undo smart-roam snr-margin** command restores the default SNR difference threshold that triggers terminal roaming.

By default, the higher and lower SNR difference thresholds that trigger terminal roaming is 15 dB and 6 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 higher SNR difference threshold that triggers terminal roaming.	The value is an integer that ranges from 10 to 20, in dB.
low-level-margin *low-level-margin*	Specifies the lower SNR difference threshold that triggers terminal roaming.	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

After smart roaming is enabled, you can run the **smart-roam snr-margin** command to set the SNR difference threshold that triggers terminal roaming. Before roaming, a STA compares the SNR of the current AP and neighboring AP and roams only when the SNR difference between the two APs is larger than the specified difference threshold.

There are two thresholds: higher and low SNR difference thresholds applicable to good and poor radio environments, respectively. A STA actively roams in good radio environments where the signal strength of the current AP is greater than or equal to 35 dB, and the SNR difference between the current AP and neighbor AP exceeds **high-level-margin**. In poor radio environments, the STA roams when the SNR of the current AP is smaller than 35 dB and the SNR difference between the current and neighbor APs is larger than **low-level-margin**.

You are advised to set **high-level-margin** larger than **low-level-margin**.

Prerequisites

The smart roaming function has been enabled using the **undo 11.2.65 smart-roam disable** command.

Example

# Set the higher and lower SNR difference thresholds that trigger terminal roaming to 10 dB and 6 dB, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] undo smart-roam disable
[HUAWEI-wlan-rrm-prof-huawei] smart-roam snr-margin high-level-margin 10 low-level-margin 6
```

11.2.75 smart-roam unable-roam-client expire-time

Function

The **smart-roam unable-roam-client expire-time** command sets the aging time of "unable to roam" record for a terminal.

The **undo smart-roam unable-roam-client expire-time** command restores the default aging time of "unable to roam" record for a terminal.

By default, the aging time of "unable to roam" record is 120 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 "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 "unable to roam" record for terminals. When the AC requests a terminal to roam but the terminal keeps sending association requests to the original AP or does not initiate an association request, the AC records the terminal as unable to roam and does not trigger terminal roaming within the specified time. After the aging time is reached, "unable to roam" record of the terminal is automatically cleared, and the system can trigger roaming of the terminal.

A terminal is recorded as unable to roam due to the following reasons:

- Due to different software configurations, some terminals preferentially send association requests to APs with which they have once associated.
- In some environments, terminals cannot scan APs with strong signals.
- Terminals enter 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 terminals 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 terminals marked unable to roam.

Prerequisites

The smart roaming function has been enabled using the **undo** **11.2.65 smart-roam disable** command.

Example

# Set the aging time of "unable to roam" record to 50 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] undo smart-roam disable
[HUAWEI-wlan-rrm-prof-huawei] smart-roam unable-roam-client expire-time 50
```

11.2.76 sta-load-balance dynamic btm-fail-times

Function

The **sta-load-balance dynamic btm-fail-times** command sets the maximum number of attempts to migrate STAs in BTM mode.

The **undo sta-load-balance dynamic btm-fail-times** command restores the default maximum number of attempts to migrate STAs in BTM mode.

By default, the maximum number of attempts to migrate 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 number of attempts to migrate 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 migrate STAs.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device preferentially uses the BTM mode to trigger STA migration to the target AP. Due to differences of STAs, some STAs can be successfully migrated 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 migrate STAs in BTM mode. If the number of attempts exceeds the specified value, the device attempts to migrate STAs in deauthentication mode.

Precautions

You are advised to retain the default value. If the success rate of STA migration in BTM mode is low, you can set a smaller value to improve the migration efficiency.

This command takes effect only in sta-number mode.

Example

# Set the maximum number of attempts to migrate 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
```

11.2.77 sta-load-balance dynamic deauth-fail-times

Function

The **sta-load-balance dynamic deauth-fail-times** command sets the maximum number of attempts to migrate STAs in deauthentication mode.

The **undo sta-load-balance dynamic deauth-fail-times** command restores the default maximum number of attempts to migrate STAs in deauthentication mode.

By default, the maximum number of attempts to migrate STAs in deauthentication mode is 2.

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 number of attempts to migrate 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 migrate 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 migration to the target AP. Due to differences of STAs, some STAs can be successfully migrated 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 migrate STAs in deauthentication mode. If the number of attempts exceeds the specified value, STAs cannot be migrated.

Precautions

You are advised to retain the default value. If the success rate of STA migration in deauthentication mode is low or STA services are affected, set the parameter value to 0 to disable STA migration in deauthentication mode.

This command takes effect only in sta-number mode.

Example

# Set the maximum number of attempts to migrate 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
```

11.2.78 sta-load-balance dynamic deny-threshold

Function

The **sta-load-balance dynamic deny-threshold** command sets the maximum number of times an AP rejects association requests of a STA for dynamic load balancing.

The **undo sta-load-balance dynamic deny-threshold** command restores the default maximum number of times an AP rejects association requests of a STA for dynamic load balancing.

By default, the maximum number of rejections is 3.

Format

sta-load-balance dynamic deny-threshold *deny-threshold*

undo sta-load-balance dynamic 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 1 to 10.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

If a STA requests to associate with an AP enabled with load balancing but the AP forbids the association according to the dynamic load balancing algorithm, the AP will reject the STA's request. However, after the number of rejections exceeds the maximum value specified by **sta-load-balance dynamic deny-threshold** command, the AP allows the STA to associate.

Example

# Set the maximum number of rejections to 8 for the terminal.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic deny-threshold 8
```

Related Topics

11.2.80 sta-load-balance dynamic sta-number gap-threshold

11.2.81 sta-load-balance dynamic sta-number start-threshold

11.2.79 sta-load-balance dynamic enable

Function

The **sta-load-balance dynamic enable** command enables the dynamic load balancing function.

The **undo sta-load-balance dynamic enable** command disables the dynamic load balancing function.

By default, the dynamic load balancing function is disabled.

Format

sta-load-balance dynamic enable

undo sta-load-balance dynamic enable

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.

In dynamic load balancing mode, a STA sends a broadcast Probe Request frame to scan available APs. The APs that receive the Probe Request frame all report the STA information to the AC. The AC adds these APs to a load balancing group, and then uses a load balancing algorithm to determine whether to allow access from the STA.

Example

# Enable dynamic load balancing.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic enable
```

11.2.80 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 based on the percentage of users is 20%.

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.
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 will count 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 **11.2.81 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.

In dynamic load balancing mode, an AC uses a load balancing algorithm to determine whether to allow a user to associate with a radio. The load balancing algorithm is as follows:

Load balancing algorithm based on the percentage of users: When implementing dynamic load balancing, the AC calculates the load percentage of each radio in a load balancing group using the formula: Load percentage of a radio = (Number of associated users on the radio/Maximum number of users allowed on the radio) x 100%. The AC compares load percentages of all radios in the load balancing group and obtains the smallest load percentage value. When a user requests to associate with an AP radio, the AC calculates the difference between the radio's load percentage and the smallest load percentage value and compares the load difference with the threshold. If the difference is smaller than the threshold, the AC allows the user to associate with the radio. If not, the AC rejects the association request of the user. If the user continues sending association requests to this AP, the AC allows the user to associate with the AP when the number of consecutive association attempts of the user exceeds the maximum number of rejection times configured using the **11.2.78 sta-load-balance dynamic deny-threshold** command on the AC.

The load balancing algorithm based on the number of users is similar to that based on the percentage of users. The only difference is that the former algorithm uses the number of users actually associated with radios to calculate the difference.

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
```

Related Topics

11.2.78 sta-load-balance dynamic deny-threshold

11.2.81 sta-load-balance dynamic sta-number start-threshold

11.2.81 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.

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
```

Related Topics

11.2.78 sta-load-balance dynamic deny-threshold

11.2.80 sta-load-balance dynamic sta-number gap-threshold

11.2.82 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 migration of the STAs.

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 migration of the STAs.

By default, the maximum number of times non-target APs suppress authentication of STAs during migration of the STAs 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 migration of the STAs.	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 migrate to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's migration 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 migration of the STAs.

Precautions

You can set a larger value of this parameter to improve the STA migration 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 migration, set a smaller value for this parameter.

This command takes effect only in sta-number mode.

Example

# Set the maximum number of times non-target APs suppress authentication of STAs during migration of the STAs 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
```

11.2.83 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 migration of the STAs.

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 migration of the STAs.

By default, the maximum number of times non-target APs suppress probing of STAs during migration of the STAs 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 migration of the STAs.	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 migrate to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's migration 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 migration of the STAs.

Precautions

You can set a larger value of this parameter to improve the STA migration 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 migration, set a smaller value for this parameter.

This command takes effect only in sta-number mode.

Example

# Set the maximum number of times non-target APs suppress probing of STAs during migration of the STAs 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
```

11.2.84 sta-load-balance dynamic steer-restrict restrict-time

Function

The **sta-load-balance dynamic steer-restrict restrict-time** command sets the duration with which non-target APs suppress association of STAs during migration of the STAs.

The **undo sta-load-balance dynamic steer-restrict restrict-time** command restores the default duration with which non-target APs suppress association of STAs during migration of the STAs.

By default, the duration with which non-target APs suppress association of STAs during migration of the STAs 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 with which non-target APs suppress association of STAs during migration of the STAs.	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 migrate to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's migration success rate. You can run the **sta-load-balance dynamic steer-restrict restrict-time** command to set the duration with which non-target APs suppress association of STAs during migration of the STAs.

Precautions

You can set a larger value of this parameter to improve the STA migration 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 migration, set a smaller value for this parameter.

This command takes effect only in sta-number mode.

Example

# Set the duration with which non-target APs suppress association of STAs during migration of the STAs 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
```

11.2.85 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 **11.2.49 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]
```

Related Topics

11.2.32 display sta-load-balance static-group

11.2.86 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
```

Related Topics

11.2.85 sta-load-balance static-group

11.2.87 sta-load-balance dynamic channel-utilization gap-threshold

Function

The **sta-load-balance dynamic channel-utilization gap-threshold** command sets the channel utilization difference threshold for load balancing in a dynamic load balancing group.

The **undo sta-load-balance dynamic channel-utilization gap-threshold** command restores the default channel utilization difference threshold for load balancing in a dynamic load balancing group.

By default, the channel utilization difference threshold for load balancing in a dynamic load balancing group is 20%.

Format

sta-load-balance dynamic channel-utilization gap-threshold *gap-threshold*

undo sta-load-balance dynamic channel-utilization gap-threshold

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold*	Specifies the channel utilization difference threshold for load balancing in a dynamic load balancing group.	The value is an integer that ranges from 1 to 99, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When dynamic load balancing based on the channel usage is implemented, an AC calculates the channel usage of each member in a dynamic load balancing group. The AC then compares the channel usage values of all members in the dynamic load balancing group and obtains the smallest channel usage value. When a STA requests to associate with an AP radio, the AC calculates the difference between the radio's channel usage and the smallest channel usage value, and compares this difference with the specified threshold. If the difference is smaller than the threshold, the AC allows the STA to associate with the radio. If not, the AC performs dynamic load balancing calculation and allows the STA to associate with the radio with a lower load.

Example

# Set the channel usage difference threshold for load balancing in the dynamic load balancing group to 30%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic channel-utilization gap-threshold 30
```

Related Topics

11.2.31 display rrm-profile

11.2.88 sta-load-balance dynamic channel-utilization start-threshold

11.2.88 sta-load-balance dynamic channel-utilization start-threshold

Function

The **sta-load-balance dynamic channel-utilization start-threshold** command sets the start threshold for dynamic load balancing based on the channel usage.

The **undo sta-load-balance dynamic channel-utilization start-threshold** command restores the default start threshold for dynamic load balancing based on the channel usage.

By default, the start threshold for dynamic load balancing based on the channel usage is 50%.

Format

sta-load-balance dynamic channel-utilization start-threshold *start-threshold*

undo sta-load-balance dynamic channel-utilization start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold*	Specifies the start threshold for dynamic load balancing based on the channel usage.	The value is an integer that ranges from 1 to 99, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the start threshold is configured for dynamic load balancing based on the channel usage, an AP calculates the channel usage of the radio with which a STA associates when the STA requests to connect to the AP. If the channel usage does not exceed the start threshold, the STA access is permitted. If the channel usage exceeds the start threshold, the AP calculates the load difference for dynamic load balancing based on the channel usage. You can run the **sta-load-balance dynamic channel-utilization gap-threshold** command to configure the load difference threshold for dynamic load balancing based on the channel usage.

Example

# Set the start threshold for dynamic load balancing based on the channel usage to 60%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic channel-utilization start-threshold 60
```

Related Topics

11.2.31 display rrm-profile

11.2.87 sta-load-balance dynamic channel-utilization gap-threshold

11.2.89 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 –70 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 –80 to –40, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

After the RSSI threshold of member devices in a dynamic load balancing group is set 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 configured RSSI threshold, the AP reports the STA information to the AC, and the AP is added to the dynamic load balancing group. Otherwise, the AP directly filters the STA information and does not report the information to the AC, and the AP will be not be 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 -65 dBm 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-threshold -65
```

11.2.90 sta-load-balance mode

Function

The **sta-load-balance mode** command configures the dynamic load balancing mode.

The **undo sta-load-balance mode** command restores the default dynamic load balancing mode.

By default, dynamic load balancing based on the number of users is used.

Format

sta-load-balance mode { **sta-number** | **channel-utilization** }

undo sta-load-balance mode

Parameters

Parameter	Description	Value
sta-number	Controls user access based on the number of users.	-
channel-utilization	Controls user access based on the channel usage.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **sta-load-balance mode** command to configure the dynamic load balancing mode based on the actual environment to provide better network experience for users.

- Dynamic load balancing based on the channel usage uses a complex algorithm but is accurately implemented to ensure service quality. This mode is recommended when service types and traffic volumes differ greatly among users.
- Dynamic load balancing based on the number of users is less accurate but uses a simple algorithm. This mode is recommended when most users have the same type of services and similar service traffic volumes.

Precautions

When configuring RUs to load balance traffic based on the channel usage, run the **ap data-collection enable** command to enable the RU data buffering function on the central AP. If this function is disabled, dynamic load balancing based on the channel usage does not take effect.

Example

# Configure dynamic load balancing based on the channel usage.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance mode channel-utilization
```

Related Topics

11.2.32 display sta-load-balance static-group

11.2.91 channel-utilization gap-threshold

Function

The **channel-utilization gap-threshold** command sets the channel usage difference threshold for load balancing in a static load balancing group.

The **undo channel-utilization gap-threshold** command restores the default channel usage difference threshold for load balancing in a static load balancing group.

By default, the channel usage difference threshold for load balancing in a static load balancing group is 20%.

Format

channel-utilization gap-threshold *gap-threshold*

undo channel-utilization gap-threshold

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold*	Specifies the channel usage difference threshold for load balancing in a static load balancing group.	The value is an integer that ranges from 1 to 99, in percentage.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When static load balancing based on the channel usage is implemented, an AC calculates the channel usage of each member in a static load balancing group. The AC then compares the channel usage values of all members in the static load balancing group and obtains the smallest channel usage value. When a STA requests to associate with an AP radio, the AC calculates the difference between the radio's channel usage and the smallest channel usage value, and compares this difference with the specified threshold. If the difference is smaller than the threshold, the AC allows the STA to associate with the radio. If not, the AC performs static load balancing calculation and allows the STA to associate with the radio with a lower load.

Example

# Set the channel usage difference threshold for load balancing in the static load balancing group to 30%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] channel-utilization gap-threshold 30
```

Related Topics

11.2.32 display sta-load-balance static-group

11.2.93 channel-utilization start-threshold

11.2.92 mode (static load balancing group view)

Function

The **mode** command configures the static load balancing mode.

The **undo mode** command restores the default static load balancing mode.

By default, static load balancing based on the number of users is used.

Format

mode { **sta-number** | **channel-utilization** }

undo mode

Parameters

Parameter	Description	Value
sta-number	Controls user access based on the number of users.	-
channel-utilization	Controls user access based on the channel usage.	-

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **mode** command to configure the static load balancing mode based on the actual environment to provide better network experience for users.

Static load balancing based on the channel usage uses a complex algorithm but is accurately implemented to ensure user experience and service quality. This mode is recommended when service types and traffic volumes differ greatly among users.

Static load balancing based on the number of users is less accurate but uses a simple algorithm. This mode is recommended when most users have the same type of services and similar service traffic volumes.

Precautions

When configuring RUs to load balance traffic based on the channel usage, run the **ap data-collection enable** command to enable the RU data buffering function on the central AP. If this function is disabled, static load balancing based on the channel usage does not take effect.

Example

# Configure static load balancing based on the channel usage.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name default
[HUAWEI-wlan-sta-lb-static-default] mode channel-utilization
```

Related Topics

11.2.32 display sta-load-balance static-group

11.2.93 channel-utilization start-threshold

Function

The **channel-utilization start-threshold** command sets the start threshold for static load balancing based on the channel usage.

The **undo channel-utilization start-threshold** command restores the default start threshold for static load balancing based on the channel usage.

By default, the start threshold for static load balancing based on the channel usage is 50%.

Format

channel-utilization start-threshold *start-threshold*

undo channel-utilization start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold*	Specifies the start threshold for static load balancing based on the channel usage.	The value is an integer that ranges from 1 to 99, in percentage.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the start threshold is configured for static load balancing based on the channel usage, an AP calculates the channel usage of the radio with which a STA associates when the STA requests to connect to the AP. If the channel usage does not exceed the start threshold, the STA access is permitted. If the channel usage exceeds the start threshold, the AP calculates the load difference for static load balancing based on the channel usage. You can run the **channel-utilization gap-threshold** command to configure the load difference threshold for static load balancing based on the channel usage.

Example

# Set the start threshold for static load balancing based on the channel usage to 60%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] channel-utilization start-threshold 60
```

Related Topics

11.2.32 display sta-load-balance static-group

11.2.91 channel-utilization gap-threshold

11.2.94 uac channel-utilization threshold

Function

The **uac channel-utilization threshold** command configures the user CAC threshold based on channel usage.

The **undo uac channel-utilization threshold** command restores the default user CAC threshold based on channel usage.

By default, the user CAC access and roaming thresholds based on channel usage are both 80%.

Format

uac channel-utilization threshold access *access-threshold* [**roam** *roam-threshold*]

undo uac channel-utilization threshold

Parameters

Parameter	Description	Value
access *access-threshold*	Specifies the user CAC access threshold based on channel usage.	The value is an integer that ranges from 1 to 100, in percentage.
roam *roam-threshold*	Specifies the user CAC roaming threshold based on channel utilization, that is, the channel utilization threshold for reassociated roaming STAs.	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

On WLANs where many users exist, such as WLANs in high density scenarios, users compete fiercely to occupy the channels 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 thresholds specified according to the radio channel usage, number of online users, or terminal SNR, which enables provisioning of high-quality network access services.

- User CAC based on channel usage uses a complex algorithm but is accurately implemented to ensure service quality. This mode is recommended when service types and traffic volumes differ greatly among users.
- User CAC based on the number of users is less accurate but 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, applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

user CAC based on channel usage and user CAC based on the number of access users cannot be configured simultaneously, but either of them can be configured together with user CAC based on terminal SNR.

Prerequisites

The user CAC function based on channel usage has been enabled using the **11.2.95 uac enable** command.

Example

# Set the user CAC access and roaming thresholds both to 50%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] uac channel-utilization enable
[HUAWEI-wlan-rrm-prof-huawei] uac channel-utilization threshold access 50 roam 50
```

Related Topics

11.2.95 uac enable

11.2.95 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** | **channel-utilization** | **client-snr** } **enable**

undo uac { **client-number** | **channel-utilization** | **client-snr** } **enable**

Parameters

Parameter	Description	Value
client-number	Controls user access based on the number of users.	-
channel-utilization	Controls user access based on channel usage.	-
client-snr	Controls user access based on 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 the channels as the number of online users increases. As a result, network quality deteriorates. To ensure network access experience of online users, configure the user Call Admission Control (CAC) function. The user CAC function allows an AP to control user access based on the thresholds specified according to the radio channel usage, number of online users, or terminal SNR, which enables provisioning of high-quality network access services.

- User CAC based on channel usage uses a complex algorithm but is accurately implemented to ensure service quality. This mode is recommended when service types and traffic volumes differ greatly among users.
- User CAC based on the number of users is less accurate but 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, applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

user CAC based on channel usage and user CAC based on the number of access users cannot be configured simultaneously, but either of them can be configured together with user CAC based on terminal SNR.

Follow-up Procedure

Run the **11.2.96 uac client-number threshold** command to configure the user CAC threshold based on the number of users or run the **11.2.94 uac channel-utilization threshold** command to configure the user CAC threshold based on channel usage.

Run the **11.2.98 uac client-snr threshold** command to configure the user CAC threshold based on the terminal SNR.

Run the **11.2.99 uac reach-access-threshold hide-ssid** command to configure the AP to automatically hide its SSID when the number of users reaches the user CAC threshold for new users.

Example

# Enable user CAC based on the number of users.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] uac client-number enable
```

Related Topics

11.2.96 uac client-number threshold

11.2.94 uac channel-utilization threshold

11.2.98 uac client-snr threshold

11.2.99 uac reach-access-threshold hide-ssid

11.2.96 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. 256	The value is an integer that ranges from 1 to 256.

Parameter	Description	Value
roam *roam-threshold*	Specifies the user CAC roaming threshold based on the number of users. This threshold is the total number of users that associated with the AP, including all local and reassociated roaming users.	The value is an integer that ranges from 1 to 256.

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 the channels 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 thresholds specified according to the radio channel usage, 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.

- User CAC based on channel usage uses a complex algorithm but is accurately implemented to ensure service quality. This mode is recommended when service types and traffic volumes differ greatly among users.
- User CAC based on the number of users is less accurate but 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, applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

user CAC based on channel usage and user CAC based on the number of access users cannot be configured simultaneously, but either of them can be configured together with user CAC based on terminal SNR.

Prerequisites

The user CAC function based on the number of users has been enabled using the **11.2.95 uac enable** command.

Example

# Set the user CAC access and roaming thresholds based on the number of users both to 50.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] uac client-number enable
[HUAWEI-wlan-rrm-prof-huawei] uac client-number threshold access 50 roam 50
```

Related Topics

11.2.95 uac enable

11.2.97 uac client-snr enable

Function

The **uac client-snr enable** command enables user CAC based on terminal SNR.

The **undo uac client-snr enable** command disables user CAC based on terminal SNR.

By default, user CAC based on terminal SNR is disabled.

Format

uac client-snr enable

undo uac client-snr enable

Parameters

None

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 the channels 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 thresholds specified according to the radio channel usage, number of online users, or terminal SNR, which enables provisioning of high-quality network access services.

- User CAC based on channel usage uses a complex algorithm but is accurately implemented to ensure service quality. This mode is recommended when service types and traffic volumes differ greatly among users.
- User CAC based on the number of users is less accurate but 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, applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

user CAC based on channel usage and user CAC based on the number of access users cannot be configured simultaneously, but either of them can be configured together with user CAC based on terminal SNR.

Follow-up Procedure

Run the **11.2.98 uac client-snr threshold** command to configure the user CAC threshold based on the terminal SNR.

Example

# Enable user CAC based on the terminal SNR.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] uac client-snr enable
```

Related Topics

11.2.98 uac client-snr threshold

11.2.98 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 20 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 75, 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 the channels 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 thresholds specified according to the radio channel usage, 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.

- User CAC based on channel usage uses a complex algorithm but is accurately implemented to ensure service quality. This mode is recommended when service types and traffic volumes differ greatly among users.
- User CAC based on the number of users is less accurate but 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, applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

user CAC based on channel usage and user CAC based on the number of access users cannot be configured simultaneously, but either of them can be configured together with user CAC based on terminal SNR.

Prerequisites

The user CAC function based on terminal SNR has been enabled using the **11.2.95 uac enable** command.

Example

# Set the user CAC threshold based on terminal SNR to 50 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] uac client-snr enable
[HUAWEI-wlan-rrm-prof-huawei] uac client-snr threshold 50
```

Related Topics

11.2.95 uac enable

11.2.99 uac reach-access-threshold hide-ssid

Function

The **uac reach-access-threshold hide-ssid** command configures SSID hiding for user CAC.

The **undo uac reach-access-threshold hide-ssid** command cancels configuration of SSID hiding for user CAC.

By default, an AP does not hide its SSID.

Format

uac reach-access-threshold hide-ssid

undo uac reach-access-threshold hide-ssid

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the user CAC function is configured, the AP denies access of new users if the number of users on the AP reaches the threshold specified for new users. To prevent new users from discovering the SSID of the AP to continue sending association requests, configure SSID hiding to disable the AP radio from advertising SSIDs of VAPs.

Prerequisites

The CAC function has been enabled using the **uac** { **client-number** | **channel-utilization** | **client-snr** } **enable** command.

Precautions

The **undo uac** { **client-number** | **channel-utilization** | **client-snr** } **enable** command disables CAC and automatically cancels SSID hiding.

Example

# Enable SSID hiding.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name huawei
[HUAWEI-wlan-rrm-prof-huawei] uac client-number enable
[HUAWEI-wlan-rrm-prof-huawei] uac reach-access-threshold hide-ssid
```

Related Topics

11.2.95 uac enable

11.3 WLAN Spectrum Analysis Configuration Commands

11.3.1 Command Support

- Only the S5720HI supports WLAN-AC commands.
- The AP3010DN-AGN and AP9330DN do not support spectrum analysis.

11.3.2 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 11-118 Description of the display spectrum-analysis server-reporter command output

Item	Description
ID	ID of the AP that reports spectrum data. To configure the AP name, run the **11.3.9 spectrum-report** command.
AP name	Name of the AP that reports spectrum data. To configure the AP name, run the **11.3.9 spectrum-report** command.
Radio ID	ID of the radio on which the function of reporting spectrum data is enabled. To set the radio ID, run the **11.3.9 spectrum-report** command.

Related Topics

11.3.9 spectrum-report

11.3.3 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. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

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 **11.3.9 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                          : 0
Detect AP name                        : 1000-0000-0011
Detect AP radio ID                    : 1
Detect AP channel                     : 149
Non-Wi-Fi device type                 : 7
Non-Wi-Fi device name                 : 5G WirelessTransmitter
Non-Wi-Fi device frequency type       : Narrow bandwidth
Non-Wi-Fi device channel              :
Non-Wi-Fi device RSSI                 :
Non-Wi-Fi device detect time last     : 1983-08-11/06:45:45
Non-Wi-Fi device center frequency(MHz) : 2422
Non-Wi-Fi device bandwidth(KHz)       : 20
Non-Wi-Fi device duty(%)              : 70
Non-Wi-Fi device interfere level      : 3
----------------------------------------------------------------
----------------------------------------------------------------
Detect AP ID                          : 1
Detect AP name                        : 1000-0000-0010
Detect AP radio ID                    : 0
Detect AP channel                     : 11
Non-Wi-Fi device type                 : 6
Non-Wi-Fi device name                 : 2.4G WirelessTransmitter
Non-Wi-Fi device frequency type       : Narrow bandwidth
Non-Wi-Fi device channel              :
Non-Wi-Fi device RSSI                 :
Non-Wi-Fi device detect time last     : 1983-08-11/01:12:25
Non-Wi-Fi device center frequency(MHz) : 2412
Non-Wi-Fi device bandwidth(KHz)       : 12
Non-Wi-Fi device duty(%)              : 94
Non-Wi-Fi device interfere level      : 3
----------------------------------------------------------------
Total: 2
```

Table 11-119 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.
Detect AP channel	ID of the AP channel on which a non-Wi-Fi device is detected.

Item	Description
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.

Related Topics

11.3.9 spectrum-report

11.3.4 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	Display information about all the non-Wi-Fi devices in the historical list.	-
ap-name *ap-name*	Display 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*	Display 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*	Display 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. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the aging time of non-Wi-Fi devices is set on the AC using the **11.3.6 spectrum-analysis non-wifi-device aging-time** command, the AC adds a non-Wi-Fi device to the historical list if an AP does not send information about the non-Wi-Fi device to the AC again.

Example

# Display information about the non-Wi-Fi devices detected by all APs in the historical list.

```
<HUAWEI> display wlan non-wifi-device history all
----------------------------------------------------------------
S/No.                                : 0
Detect AP name                       : huawei
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 11-120 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	Type of the detected non-Wi-Fi device.
Non-Wi-Fi device type	ID of the AP channel on which a non-Wi-Fi device is detected.
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.
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.

Related Topics

11.3.6 spectrum-analysis non-wifi-device aging-time

11.3.5 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 some APs of the WLAN 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 so that radio calibration can be implemented.

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
```

11.3.6 spectrum-analysis non-wifi-device aging-time

Function

The **spectrum-analysis non-wifi-device aging-time** command configures the aging time of non-Wi-Fi devices on the AC during spectrum analysis.

The **undo spectrum-analysis non-wifi-device aging-time** command restores the default aging time of non-Wi-Fi devices on the AC during spectrum analysis.

By default, the aging time of non-Wi-Fi devices on the AC 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 of non-Wi-Fi devices on the AC.	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 the AC is configured as the spectrum analysis server using the **11.3.7 spectrum-analysis server** command, the AC stores information about analyzed non-Wi-Fi devices. If an AP does not report information about a non-Wi-Fi device to the AC 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 **11.3.4 display wlan non-wifi-device history** command to check information about non-Wi-Fi devices in the historical list.

Precautions

Currently, the AC cannot identify different devices of the same type. For example, when the AC detects two bluetooth devices: A and B, the AC can only record the devices as a bluetooth device and update the detection time of the bluetooth device.

Example

# Set the aging time of non-Wi-Fi devices on the AC 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
```

Related Topics

11.1.120 display ap-system-profile

11.3.4 display wlan non-wifi-device history

11.3.7 spectrum-analysis server

11.3.7 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.

Parameter	Description	Value
port *port-number*	Specifies the port number (UDP port number) of a spectrum server.	The value is an integer that ranges from 5000 to 65535. **NOTE** The port number of eSight is 32181.
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, specify a valid IP address and port number for the spectrum server (The specified values do not take effect.) and configure the **via-ac ac-port** *ac-port-number* command.

Example

# Set the IP address and port number of a spectrum server to 10.137.43.4 and 32181.

```
<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 32181
```

Related Topics

11.1.120 display ap-system-profile

11.3.9 spectrum-report

11.3.8 spectrum-analysis source

Function

The **spectrum-analysis source** command configures the source IP address of packets sent by an AC to a spectrum server.

The **undo spectrum-analysis source** command deletes the configured source IP address of packets sent by an AC to a spectrum server.

By default, an 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 an 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, an 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 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
```

11.3.9 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 already exist.
ap-id *ap-id*	Specifies an AP ID. The AP ID and radio ID identify a radio.	The AP ID must already exist.
radio *radio-id*	Specifies a radio ID.	The value is an integer that ranges from 0 to 2. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.
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 **11.3.5 spectrum-analysis enable** command.

Follow-up Procedure

Run the **11.3.7 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 a restart and needs to be configured again.

Example

# Enable the function of reporting spectrum data on radio 0 of AP **ap-huawei**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] spectrum-report ap-name ap-huawei radio 0
```

Related Topics

11.3.5 spectrum-analysis enable

11.3.7 spectrum-analysis server

11.3.10 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 already exist.
ap-id *ap-id*	Clears information about the non-Wi-Fi devices detected by a specified AP ID.	The AP ID must already exist.
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. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting information about detected non-Wi-Fi devices in a period, you can run the reset command to clear existing information so that the AC can recollect 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 use the reset command. After the command is run, you can run the **11.3.4 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
```

Related Topics

11.3.4 display wlan non-wifi-device history

11.3.11 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. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **reset wlan non-wifi-device history** command clears 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
```

Related Topics

11.3.3 display wlan non-wifi-device

11.3.4 display wlan non-wifi-device history

11.4 WLAN Roaming Commands

11.4.1 Command Support

Only the S5720HI supports WLAN-AC commands.

11.4.2 beacon disable

Function

The **beacon disable** command disables RUs from sending Beacon frames.

The **undo beacon disable** command enables RUs to send Beacon frames.

By default, RUs are enabled to send Beacon frames.

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 RUs from sending Beacon frames may cause STAs to go offline due to a failure to receive Beacon frames.

Example

# Disable RUs 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
```

Related Topics

11.4.8 sfn-roam enable

11.4.3 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
```

Related Topics

11.4.8 sfn-roam enable

11.4.4 cts disable

11.4.4 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.

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
```

Related Topics

11.4.8 sfn-roam enable

11.4.5 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 STAs associated with a central AP is displayed.
- If an AP name or ID is specified, roaming statistics about all STAs associated with the AP is displayed.

Example

# Display roaming statistics about all STAs.

```
<HUAWEI> display station roam-statistics
--------------------------------------------------------------------------------
 Online stations                                          :0
 Online roaming stations                                      :0
--------------------------------------------------------------------------------
```

Table 11-121 Description of the **display station roam-statistics** command output

Item	Description
Online stations	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 stations                                          :0
 Online roaming stations                                      :0
----------------------------------------------------------------------------
```

Table 11-122 Description of the **display station roam-statistics** *ap-name* command output

Item	Description
Online stations	Number of online STAs.
Online roaming stations	Number of online roaming STAs.

11.4.6 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 four 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 0011-43c7-d73e.

```
<HUAWEI> display station roam-track sta-mac 0011-43c7-d73e
Access SSID:huawei
Rx/Tx:link receive rate/link transmit rate(Mbps)
c:PMK Cache Roam r:802.11r Roam s:Same Frequency Network
------------------------------------------------------------------------------
L2/L3           AC IP                   AP name             Radio ID
BSSID           TIME                    In/Out RSSI         Out Rx/Tx
------------------------------------------------------------------------------
--              192.168.109.1           Huawei1             1
dcd2-fc9d-0bb0  2015/01/12 16:52:58   -51/-48               46/13
L2              192.168.109.1           Huawei2             1
e468-a34d-afb0  2015/01/12 16:55:45   -58/-                 -/-
------------------------------------------------------------------------------
Number: 1
```

Table 11-123 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	Whether a STA roams at Layer 2 or Layer 3. ● c: PMK cache roam. ● r: 802.11r roam. ● s: Agile distributed single frequency network (SFN) roaming.
AC IP	IP address of an AC that the STA has associated with.
AP name	Name of an AP that the STA has associated with.

Item	Description
Radio ID	ID of a radio that the STA has associated with.
BSSID	BSSID of an AP that the STA has associated with.
TIME	Time duration when the STA has associated with an AP.
In/Out RSSI	RSSI of the AP that the STA has 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.

11.4.7 dot11r enable

Function

The **dot1r enable** command enables 802.11.1r.

The **undo dot11r enable** command disables 802.11.1r.

By default, 802.11r is disabled.

Format

dot11r enable [**reassociate-timeout** *time*]

undo dot11r enable

Parameters

Parameter	Description	Value
reassociate-timeout *time*	STA re-association timeout period.	The value is an integer that ranges from 1 to 10, in seconds. The default value is 1.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During roaming, the STA needs to be re-authenticated 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 the network delay.

Precautions

- IEEE 802.11r supports open system, WPA2-PSK, and 802.1x authentication.
- The 802.11r fast roaming and Protected Management Frame (PMF) functions are mutually exclusive. If the 802.11r fast roaming function has been configured, the PMF function cannot be configured.

Example

# Enable 802.11r.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dot11r enable
```

11.4.8 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.

Precautions

- Network planning precautions:
  - Agile distributed SFN roaming is supported only by the AD9430DN-12 (including matching RUs) and AD9430DN-24 (including matching RUs). RUs support agile distributed SFN roaming in the following combination modes:
    - Between the R230D and R240D (Note: Only the 2.4 GHz radio of the R230D and R240D supports agile distributed SFN roaming, and the 5 GHz radio does not support.)
    - Among the R250D, R250D-E, and R450D
  - For the central AP, after agile distributed SFN roaming is enabled, the total number of agile distributed SFN roaming STAs on a single frequency band (2.4 GHz or 5 GHz) of all RUs does not exceed 128, and that of STAs associated with other VAPs on the same band does not exceed 128.
  - After agile distributed SFN roaming is enabled, configure all RUs to work on the same channel. When agile distributed SFN roaming is enabled on the 5 GHz frequency band, configure non-radar channels.
  - RUs involved in roaming must be associated with the same central AP but do not support agile distributed SFN roaming between central APs.
  - Inter-RU roaming is Layer 2 roaming within a central AP. Agile distributed SFN roaming is not performed on Layer 3.
- Configuration precautions:
  - When agile distributed SFN roaming is enabled for both the 2.4 GHz and 5 GHz radios, it is recommended that different SSIDs be used. Otherwise, the radio switchover may occur, affecting user experience.
  - Agile distributed SFN roaming can be enabled only on one VAP of a radio. If multiple VAPs are configured on a radio, it is recommended that the total VAP rate limit on all VAPs with agile distributed SFN roaming disabled be set to 5 Mbit/s.
  - Radios enabled with agile distributed SFN roaming do not support channel scanning, channel calibration, or smart roaming.
  - Agile distributed SFN roaming can be configured based only on AP groups but not based on APs.
  - RUs involved in agile distributed SFN roaming need to have the following items configured the same:
    - SSID
    - VAP profile and VAP ID
    - Security policy. Agile distributed SFN roaming supports these encryption modes: WPA+PSK, WPA2+PSK, WPA-WPA2+PSK, WPA

+802.1X (EAP authentication), WPA2+802.1X (EAP authentication), WPA-WPA2+802.1X (EAP authentication), and Portal+PSK.

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
```

11.4.9 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 the slow roaming switchover, affecting user experience. A small value causes frequent roaming switchovers, 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
```

Related Topics

11.4.8 sfn-roam enable

11.4.11 sfn-roam roam-check check-interval

11.4.10 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 switchover 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 the slow roaming switchover, affecting user experience. A small value causes frequent roaming switchovers, 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
```

Related Topics

11.4.8 sfn-roam enable

11.4.11 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 the slow roaming switchover, affecting user experience. A small value causes frequent roaming switchovers, 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
```

Related Topics

11.4.8 sfn-roam enable

11.4.9 sfn-roam report-interval

11.4.12 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 switchover occurs when the RSSI gap between the local RU and a surrounding RU reaches the specified value. A large value causes the slow roaming switchover, affecting user experience. A small value causes frequent roaming switchovers, 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
```

Related Topics

11.4.8 sfn-roam enable

11.4.13 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 switchover 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
```

Related Topics

11.4.8 sfn-roam enable

11.4.14 sfn-roam roam-check low-threshold

11.4.14 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 switchover 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
```

Related Topics

11.4.8 sfn-roam enable

11.4.13 sfn-roam roam-check high-threshold

11.4.15 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 switchover occurs when the cumulative RSSI change value reaches the specified threshold. A large value causes the slow roaming switchover, affecting user experience. A small value causes frequent roaming switchovers, 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
```

Related Topics

11.4.8 sfn-roam enable

11.4.16 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 switchovers, you can specify a proper number of STA holding times. A large value causes the slow roaming switchover, affecting user experience. A small value causes frequent roaming switchovers, 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
```

Related Topics

11.4.8 sfn-roam enable

11.5 WLAN QoS Configuration Commands

11.5.1 Command Support

Only the S5720HI supports WLAN-AC commands.

11.5.2 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.

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
```

Related Topics

11.2.53 rrm-profile (WLAN view)

11.5.3 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
```

Related Topics

11.5.26 ucc-profile (system view)

11.5.6 display ucc-profile

11.5.4 display references traffic-profile

Function

The **display references traffic-profile** command displays the reference information of a traffic profile.

Format

display references traffic-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays the reference information of 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 the reference information of the traffic profile **p1**.

```
<HUAWEI> display references traffic-profile name p1
---------------------------------------------------
Reference type    Reference name
---------------------------------------------------
VAP profile       default
VAP profile       wlan-vap
VAP profile       jsl
VAP profile       test
VAP profile       wlan-vap1
VAP profile       huawei
VAP profile        2
----------------------------------------------------
Total: 7
```

Table 11-124 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.

11.5.5 display traffic-profile

Function

The **display traffic-profile** command displays configuration information about a traffic profile.

Format

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

Parameters

Parameter	Description	Value
all	Displays configuration information about all traffic profiles.	-
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 double quotation marks (" ").

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display traffic-profile** command to check 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                                          : 1
Priority map downstream trust                       : DSCP
User isolate mode                                   : disable
Rate limit client up(Kbps)                          : 4294967295
Rate limit client down(Kbps)                        : 4294967295
Rate limit VAP up(Kbps)                             : 4294967295
Rate limit VAP down(Kbps)                           : 4294967295
IGMP snooping                                       : disable
IGMP snooping report suppress                       : disable
Spectralink voice priority                          : disable
Priority map upstream trust                         : 8021e
IGMP snooping max bandwith(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
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 Type                Direction  RemarkType  RemarkValue  AppliedRecord
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
```

# Display configuration information about a traffic profile that maps the trusted DSCP 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                                  : 1
Priority map downstream trust                       : DSCP
User isolate mode                                : disable
Rate limit client up(Kbps)                        : 4294967295
Rate limit client down(Kbps)                       : 4294967295
Rate limit VAP up(Kbps)                          : 4294967295
Rate limit VAP down(Kbps)                         : 4294967295
IGMP snooping                                    : disable
IGMP snooping report suppress                       : disable
Spectralink voice priority                        : disable
Priority map upstream trust                        : 8021e
IGMP snooping max bandwith(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                 : DSCP
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
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
priority upstream map mode      : DSCP map DSCP
                    0 map 0
                    1 map 1
                    2 map 2
                    3 map 3
                    4 map 4
                    5 map 5
                    6 map 6
                    7 map 7
                    8 map 8
                    9 map 9
                    10 map 10
                    11 map 11
                    12 map 12
                    13 map 13
                    14 map 14
                    15 map 15
                    16 map 16
                    17 map 17
                    18 map 18
                    19 map 19
                    20 map 20
                    21 map 21
                    22 map 22
                    23 map 23
                    24 map 24
                    25 map 25
                    26 map 26
                    27 map 27
                    28 map 28
                    29 map 29
                    30 map 30
                    31 map 31
                    32 map 32
                    33 map 33
                    34 map 34
                    35 map 35
                    36 map 36
                    37 map 37
                    38 map 38
                    39 map 39
                    40 map 40
                    41 map 41
                    42 map 42
                    43 map 43
                    44 map 44
                    45 map 45
                    46 map 46
                    47 map 47
                    48 map 48
                    49 map 49
                    50 map 50
                    51 map 51
                    52 map 52
                    53 map 53
                    54 map 54
                    55 map 55
                    56 map 56
                    57 map 57
                    58 map 58
                    59 map 59
                    60 map 60
                    61 map 61
                    62 map 62
                    63 map 63
```

```
priority tunnel upstream map mode  : DSCP map 802.1p
                                      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
------------------------------------------------------------------------------------------
Traffic Type                         Direction  AppliedRecord
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------
Traffic Type                         Direction  RemarkType  RemarkValue  AppliedRecord
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

Table 11-125 Description of the **display traffic-profiledisplay wlan traffic-profile** command output

Item	Description
Profile ID	Traffic profile ID
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 the parameter, run the **11.5.12 priority-map downstream trust** command.
User isolate mode	User isolation. To configure the parameter, run the **11.5.28 user-isolate (traffic profile view)** command.
Rate limit client up(Kbps)	Indicates upstream rate limit configured for STAs. To configure the parameter, run the **11.5.20 rate-limit** command.
Rate limit client down(Kbps)	Indicates downstream rate limit configured for STAs. To configure the parameter, run the **11.5.20 rate-limit** command.
Rate limit VAP up(Kbps)	Indicates upstream rate limit configured for VAPs. To configure the parameter, run the **11.5.20 rate-limit** command.

Item	Description
Rate limit VAP down(Kbps)	Indicates downstream rate limit configured for VAPs. To configure the parameter, run the **11.5.20 rate-limit** command.
Traffic optimize sta bridge forward	Function of forbidding STA bridging packet forwarding.
IGMP snooping	IGMP snooping.
Spectralink voice priority	SVP voice traffic optimization. To configure this parameter, run the **11.5.21 svp-voice enable** command.
IGMP snooping report suppress	IGMP message suppression time.
IGMP snooping max bandwith(kbps)	Maximum multicast bandwidth of a VAP. To configure this parameter, run the **11.12.4 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 **11.12.5 igmp-snooping max-user (traffic profile view)** command.
Traffic optimize broadcast suppression(pps)	Maximum broadcast traffic volume allowed on an interface. To configure the parameter, run the **11.12.8 traffic-optimize broadcast-suppression** command.
Traffic optimize multicast suppression(pps)	Maximum multicast traffic volume allowed on an interface. To configure the parameter, run the **11.12.9 traffic-optimize multicast-suppression** command.
Traffic optimize unicast suppression(pps)	Maximum unicast traffic volume allowed on an interface. To configure the parameter, run the **11.12.13 traffic-optimize unicast-suppression** command.

Item	Description
Traffic optimize multicast to unicast	Function of converting multicast packets to unicast packets. To configure the parameter, run the **11.12.10 traffic-optimize multicast-unicast enable** command.
Dynamic adaptive	Whether to enable adaptive multicast-to-unicast conversion. To configure this function, run the **11.12.11 traffic-optimize multicast-unicast dynamic-adaptive disable** command.
CAPWAP priority upstream map mode	Mapping from WMM to the DSCP priority of the upstream CAPWAP tunnel.
Priority map tunnel upstream trust	Trusted priority for mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP. To configure the parameter, run the **11.5.17 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 **11.5.18 priority-map upstream trust** command.
WMM priority downstream map mode	Mapping from the DSCP priority to the WMM of downstream packets.
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 of packets to be filtered. To configure this parameter, run the **11.5.22 traffic-filter (traffic profile view)** command.
AppliedRecord(Traffic Type: traffic-filter)	ACL-based packet filtering records. To configure this parameter, run the **11.5.22 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 **11.5.25 traffic-remark (traffic profile view)** command.
RemarkType	Packet priority re-marking type. To configure this parameter, run the **11.5.25 traffic-remark (traffic profile view)** command.
RemarkValue	Re-marked packet priority value. To configure this parameter, run the **11.5.25 traffic-remark (traffic profile view)** command.
AppliedRecord(Traffic Type: traffic-remark)	ACL-based packet priority re-marking record. To configure this parameter, run the **11.5.25 traffic-remark (traffic profile view)** command.

# Display configurations of all traffic profiles.

```
<HUAWEI> display traffic-profile all
----------------------------------------------------
Profile name                 Reference
----------------------------------------------------
default                       3
1                            1
p1                           0
----------------------------------------------------
Total: 3
```

Table 11-126 Description of the **display traffic-profile alldisplay wlan traffic-profile all** command output

Item	Description
Profile name	Profile name. To configure the parameter, run the **11.5.23 traffic-profile (WLAN view)** command.
Reference	Number of times a location profile is referenced.

Related Topics

11.5.23 traffic-profile (WLAN view)

11.5.6 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 11-127 Description of the **display ucc-profile all** command output

Item	Description
Profile name	Name of the UCC profile.

Item	Description
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 11-128 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.

Related Topics

11.5.26 ucc-profile (system view)

11.5.7 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
```

Related Topics

11.5.26 ucc-profile (system view)

11.5.6 display ucc-profile

11.5.8 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
```

Related Topics

14.1.5 acl (system view)

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

11.5.9 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
```

11.5.10 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 802.11 user priority.	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 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
```

Related Topics

11.5.23 traffic-profile (WLAN view)

11.5.5 display traffic-profile

11.5.11 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 11-129 describes the default mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets.

Table 11-129 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. The value of *dscp-value2* must be larger than that of *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 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
```

Related Topics

11.5.23 traffic-profile (WLAN view)

11.5.5 display traffic-profile

11.5.12 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 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
```

Related Topics

11.5.23 traffic-profile (WLAN view)

11.5.5 display traffic-profile

11.5.13 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 11-130 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 11-130 Default mapping from the user priority of 802.11 packets to the DSCP priority in the CAPWAP header

User Priority of 802.11 Packets	DSCP Priority in the CAPWAP Header
0	0
1	8
2	16
3	24

User Priority of 802.11 Packets	DSCP Priority in the CAPWAP Header
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. The value of *dot11e-value2* must be larger than that of *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**, configures 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
```

Related Topics

11.5.5 display traffic-profile

11.5.23 traffic-profile (WLAN view)

11.5.14 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 802.11 user priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
to *dot11e-value2*	Specifies the 802.11 user priority.	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 in a tunnel packet.	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
```

Related Topics

11.5.5 display traffic-profile

11.5.23 traffic-profile (WLAN view)

11.5.15 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 11-131 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 11-131 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 in a tunnel packet.	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
```

Related Topics

11.5.5 display traffic-profile

11.5.23 traffic-profile (WLAN view)

11.5.16 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.
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. The value of *dscp-value1* must be larger than that of *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**, configures 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
```

Related Topics

11.5.5 display traffic-profile

11.5.23 traffic-profile (WLAN view)

11.5.17 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
```

Related Topics

11.5.23 traffic-profile (WLAN view)

11.5.5 display traffic-profile

11.5.18 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 802.11p 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 11-132 Mapping between the DSCP and 802.11p 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

DSCP Priority of 802.11 Packets	802.1p Priority of 802.3 Packets
56-63	7

Table 11-133 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
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
```

Related Topics

11.5.23 traffic-profile (WLAN view)

11.5.5 display traffic-profile

11.5.19 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 an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through.	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.

Parameter	Description	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.

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
```

11.5.20 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 limited rate of packets.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.

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.

Example

# Set the limited rate 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
```

Related Topics

11.5.23 traffic-profile (WLAN view)

11.5.5 display traffic-profile

11.5.21 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
```

11.5.22 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 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 acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } **ipv4 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.	-

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. ● 3000 to 3031: advanced ACLs ● 6000 to 6031: user ACLs
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* indicates an ACL name.	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.

- **14.1.5 acl (system view)**
- **14.1.4 acl name**

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
```

11.5.23 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 enter the traffic profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1]
```

Related Topics

11.5.5 display traffic-profile

11.5.24 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 **11.5.23 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
```

Related Topics

11.5.23 traffic-profile (WLAN view)

11.5.5 display traffic-profile

11.5.25 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 acl** { *acl-number* | **name** *acl-name* } { **dot11e** *dot11e-value* | **dscp** *dscp-value* }

undo traffic-remark { **inbound** | **outbound** } **ipv4 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.	-
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. ● 3000 to 3031: advanced ACLs ● 6000 to 6031: user ACLs

Parameter	Description	Value
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* mapping *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.

- **14.1.5 acl (system view)**
- **14.1.4 acl 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 **11.5.22 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
```

11.5.26 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]
```

Related Topics

11.5.6 display ucc-profile

11.5.27 ucc-profile (VAP profile view)

11.5.27 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
```

Related Topics

11.1.152 display vap-profile

11.5.26 ucc-profile (system view)

11.5.6 display ucc-profile

11.5.28 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 a 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
```

11.5.29 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
```

Related Topics

11.5.26 ucc-profile (system view)

11.5.6 display ucc-profile

11.5.30 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
```

Related Topics

11.5.26 ucc-profile (system view)

11.5.6 display ucc-profile

11.5.31 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 11-134 lists the default EDCA parameter settings and ACK policies for APs.

Table 11-134 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.	-

Parameter	Description	Value
aifsn *aifsn-value*	Specifies the AIFSN, which determines the channel idle time.	The value is an integer that ranges from 1 to 15.
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 be smaller 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-value*. The value 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 to the packets. In this way, APs have different capabilities to compete for channels and provide 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 11-135** lists the reference EDCA parameter settings and ACK policies for APs in voice scenarios.

Table 11-135 Reference EDCA parameter settings and ACK policies for APs 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 11-136** lists the reference EDCA parameter settings and ACK policies for APs in voice and video scenarios.

Table 11-136 Reference EDCA parameter settings and ACK policies for APs 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

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
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
```

11.5.32 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 11-137 lists the default EDCA parameter settings for STAs.

Table 11-137 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.	-
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 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 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. **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 11-138 describes the EDCA parameters.

Table 11-138 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 11-139** lists the reference EDCA parameter settings and ACK policies for APs in voice scenarios.

Table 11-139 Reference EDCA parameter settings and ACK policies for APs 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 11-140 lists the reference EDCA parameter settings and ACK policies for APs in voice and video scenarios.

Table 11-140 Reference EDCA parameter settings and ACK policies for APs 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
```

Related Topics

11.1.143 display ssid-profile

11.5.33 wmm disable

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

802.11n and 802.11ac STAs must support WMM. If the WMM function is disabled in a radio, 802.11n and 802.11ac 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
```

Related Topics

11.1.219 radio-2g-profile (WLAN view)

11.1.221 radio-5g-profile (WLAN view)

11.5.34 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
```

11.6 WLAN Location Configuration Commands

NOTE

- Only the R250D-E, AP2050DN-E, AP4050DN-E, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP8050DN, AP8050DN-S, AP8150DN, and AP7050DE support Bluetooth location, Bluetooth tag location and Bluetooth data transparent transmission. Only the AP4050DN-E supports the Bluetooth broadcast function.

11.6.1 Command Support

- Only the S5720HI supports WLAN-AC commands.
- The AP9330DN does not support the WLAN tag location function.
- The AP3010DN-AGN, AP6310SN-GN, and AP9330DN do not support the WLAN terminal location function.
- Only the R250D-E, AP2050DN-E, AP4050DN-E, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN, AP8050DN, AP8050DN-S, AP8150DN, and AP7050DE support Bluetooth location, Bluetooth tag location and Bluetooth data transparent transmission. Only the AP4050DN-E supports the Bluetooth broadcast function.

11.6.2 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 huawei
[HUAWEI-wlan-location-prof-huawei] aeroscout compound-time 100
```

Related Topics

11.6.17 display location-profile

11.6.3 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 huawei
[HUAWEI-wlan-location-prof-huawei] aeroscout mu-enable
```

Related Topics

11.6.17 display location-profile

11.6.4 aeroscout server

Function

The **aeroscout server** command sets the destination IP address and port number on the AeroScout server for APs to report location packets of AeroScout tags and Mobile Units (MUs).

The **undo aeroscout server** command deletes the configured destination IP address and port number on the AeroScout server for APs to report location packets of AeroScout tags and MUs.

By default, destination IP address or 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 the destination port number on the AeroScout location server to which APs directly report location packets of AeroScout tags and MUs. Specifies the destination port number on the AeroScout location server to which the AC reports location packets of AeroScout tags and MUs through an AC.	The value is an integer that ranges from 1025 to 65535.
via-ac	Specifies that the tag packets received by APs are reported to the AeroScout location server through an AC. **NOTE** If the APs directly report the received tag and MU packets to the AeroScout location server, the **11.6.24 display wlan location statistics aeroscout** command cannot display location statistics about the AeroScout tags and MUs.	-
ac-port *ac-port-num*	Indicates 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 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 configured in the current location profile for a specific location method, it cannot be configured in other profiles for the same location method.

NOTE

The AeroScout location server actively sets up connections with APs. You need to manually add APs and specify the APs' MAC addresses, port numbers, and IP addresses on the AeroScout location server. If APs report location packets through the AC, you also need to specify the AC's IP address. You do not need to specify the IP address of the AeroScout server on the AC.

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 huawei
[HUAWEI-wlan-location-prof-huawei] aeroscout server port 1144
```

Related Topics

11.6.17 display location-profile

11.6.5 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 huawei
[HUAWEI-wlan-location-prof-huawei] aeroscout tag-enable
```

Related Topics

11.6.17 display location-profile

11.6.6 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 **11.6.39 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
```

Related Topics

11.6.39 sniffer enable

11.6.7 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 mac *mac-address1* [**to** *mac-address2*]

undo ble monitoring-list [**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.

Parameter	Description	Value
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 equal to or larger than the *mac-address1* value. *mac-address1* and *mac-address2* jointly specify a range of MAC addresses.	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

After the Bluetooth monitoring, Bluetooth tag location, or Bluetooth data transparent transmission function is enabled using the **11.6.39 sniffer enable** command, all Bluetooth devices are monitored when no Bluetooth device (BLE device, Bluetooth tag, or Bluetooth client) is added to the monitoring list. When any Bluetooth device is offline or has insufficient battery power, an alarm is triggered on the AC accordingly. When 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 AC accordingly. Bluetooth clients do not support low power alarms.

Precautions

After the BLE monitoring, Bluetooth tag location, or Bluetooth data transparent transmission function is disabled using the **undo 11.6.39 sniffer enable** command, an alarm is triggered on the AC 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 MAC address 1234-1234-1000 to the monitoring list.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble monitoring-list mac 1234-1234-1000
```

# Add Bluetooth devices with MAC addresses 1234-1234-1000 to 1234-1234-1006 to the monitoring list.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble monitoring-list mac 1234-1234-1000 to 1234-1234-1006
```

Related Topics

11.6.21 display wlan ble site-info

11.6.39 sniffer enable

11.6.8 ble report

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 *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 Bluetooth device information is deleted and the AP collects information about new Bluetooth devices. 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
```

Related Topics

11.6.21 display wlan ble site-info

11.6.9 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
```

11.6.10 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 **11.6.11 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 **huawei** and bind the profile to AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name huawei
[HUAWEI-wlan-ble-prof-huawei] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] ble-profile huawei
```

Related Topics

11.1.36 ap-group

11.6.11 ble-profile (WLAN view)

11.6.18 display references ble-profile

11.6.11 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 **11.6.10 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 **huawei** and enter its view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name huawei
[HUAWEI-wlan-ble-prof-huawei]
```

Related Topics

11.6.16 display ble-profile

11.6.10 ble-profile (AP group view and AP view)

11.6.12 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

Only the AP4050DN-E supports the Bluetooth broadcast function.

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 huawei
[HUAWEI-wlan-ble-prof-huawei] broadcaster enable
```

Related Topics

11.6.16 display ble-profile

11.6.13 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

Only the AP4050DN-E supports the Bluetooth broadcast function.

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

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.

Parameter	Description	Value
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 BEL 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 BEL 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 BEL 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 BEL 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 BEL 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 BEL 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 **11.6.12 broadcaster enable** command, you can run the **broadcasting-content** 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 **11.6.42 tx-power (BLE profile view)** command, you need to remeasure and reconfigure the RSSI calibration value. Therefore, you are advised to run the **11.6.42 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 huawei
[HUAWEI-wlan-ble-prof-huawei] broadcasting-content uuid uuid-hex 12345678123456789 major major-hex A22 minor minor-hex 011 reference-rssi -70
```

Related Topics

11.6.12 broadcaster enable

11.6.16 display ble-profile

11.6.42 tx-power (BLE profile view)

11.6.14 broadcasting-content (AP group view and AP view)

Function

The **broadcasting-content uuid** command sets a universally unique identifier (UUID) of the Bluetooth Low Energy (BLE) broadcast frames sent by an AP's built-in Bluetooth module.

The **undo broadcasting-content uuid** command restores the UUID of the BLE broadcast frames sent by an AP's built-in Bluetooth module to the default value.

By default, the UUID of the BLE broadcast frames sent by an AP's built-in Bluetooth module is null.

NOTE

Only the AP4050DN-E supports the Bluetooth broadcast function.

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 digits.

Views

AP group view and 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 **11.6.12 broadcaster enable** command, you can run the **broadcasting-content uuid** command to set a UUID of the BLE broadcast frames. If you do not want to set a UUID of BLE broadcast frames in a BLE profile, set it in the AP group view or AP view.

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 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
```

Related Topics

11.6.12 broadcaster enable

11.1.119 display ap-group

11.1.91 display ap config-info

11.6.15 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

Only the AP4050DN-E supports the Bluetooth broadcast function.

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 **11.6.12 broadcaster enable** command, you can run the **broadcasting-interval** 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 huawei
[HUAWEI-wlan-ble-prof-huawei] broadcasting-interval 1000
```

Related Topics

11.6.12 broadcaster enable

11.6.16 display ble-profile

11.6.16 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 a BLE profile.

Example

# Display information about all BLE profiles.

```
<HUAWEI> display ble-profile all
----------------------------------------------------------------------------
Profile name                      Reference
----------------------------------------------------------------------------
huawei                            1
----------------------------------------------------------------------------
Total: 1
```

Table 11-141 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 BLE profile **huawei**.

```
<HUAWEI> display ble-profile name huawei
------------------------------------------------------------------------------
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 11-142 Description of the **display ble-profile name** *profile-name* command output

Item	Description
Broadcaster switch	Whether the Bluetooth broadcast function is enabled. The options are as follows: ● enable: The Bluetooth broadcast function is enabled. ● disable: The Bluetooth broadcast function is disabled. To configure this parameter, run the **11.6.12 broadcaster enable** command.
Broadcaster interval(ms)	Interval at which BLE broadcast frames are sent. To configure this parameter, run the **11.6.15 broadcasting-interval** command.
Broadcaster content	Content of a BLE broadcast frame. To configure this parameter, run the **11.6.13 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 Bluetooth device, for example, location of a Bluetooth 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 Bluetooth device, for example, location of a Bluetooth device.
Reference RSSI	RSSI calibration value. RSSI calibration value refers to the RSSI of a Bluetooth device measured at a distance of 1 m. It is used to calculate the distance between a Bluetooth device and a Bluetooth terminal or tag.

Item	Description
Transmit power	Transmit power of an AP's built-in Bluetooth module. To configure this parameter, run the **11.6.42 tx-power (BLE profile view)** command.
Sniffer switch	Whether the Bluetooth function is enabled. The options are as follows: ● enable: The Bluetooth function is enabled. ● disable: The Bluetooth function is disabled. To configure this parameter, run the **11.6.39 sniffer enable** command.
Source IP address	Source IP address used by an AC to report BLE packets. To configure the parameter, run the **11.6.41 source (BLE profile view)** command.
Sniffer mode	Working mode of an AP's built-in Bluetooth module. To configure this parameter, run the **11.6.39 sniffer enable** command.
Report switch	Whether an AP is enabled to send Bluetooth packets. The options are as follows: ● enable: An AP is enabled to send Bluetooth packets. ● disable: An AP is disabled from sending Bluetooth packets. To configure this parameter, run the **11.6.34 report enable** command.
Report mode	Mode in which an AP sends Bluetooth packets. To configure this parameter, run the **11.6.35 report-mode** command.
Report interval(s)	Interval at which an AP sends Bluetooth packets. To configure this parameter, run the **11.6.35 report-mode** command.
Report server	IP address of a Bluetooth server. To configure this parameter, run the **11.6.36 report-to-server** command.

Item	Description
Report server port	Destination port number on a server to which Bluetooth packets are sent. To configure this parameter, run the **11.6.36 report-to-server** command.
Report via-AC	Whether Bluetooth packets are sent to a server through an AC. The options are as follows: ● enable: Bluetooth packets are sent to a server through an AC. ● disable: Bluetooth packets are sent directly to a server. To configure this parameter, run the **11.6.36 report-to-server** command.
Report via-AC port	Number of the port on an AC through which an AP sends Bluetooth packets. To configure this parameter, run the **11.6.36 report-to-server** command.

Related Topics

11.6.11 ble-profile (WLAN view)

11.6.12 broadcaster enable

11.6.13 broadcasting-content

11.6.15 broadcasting-interval

11.6.39 sniffer enable

11.6.42 tx-power (BLE profile view)

11.6.17 display location-profile

Function

The **display location-profile** command displays configuration information about a location profile.

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

Format

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

display references location-profile 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
location-profile-1                 0
location-profile-2                 10
----------------------------------------------------------
Total: 3
```

Table 11-143 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 port           : -
private via-AC                : disable
private via-AC port           : -
private report-frequency(ms)  : 20000
private mu protocol-version   : v3
------------------------------------------------------------
```

Table 11-144 Description of the **display location-profile name default** command output

Item	Description
Aeroscout-tag	Whether WLAN location of AeroScout tags is enabled. ● enable: The function is enabled. ● disable: The function is disabled. To configure the function, run the **11.6.5 aeroscout tag-enable** command.
Aeroscout-mu	Whether WLAN location of AeroScout MUs is enabled. ● enable: The function is enabled. ● disable: The function is disabled. To configure the function, run the **11.6.3 aeroscout mu-enable** command.
Aeroscout ae-port	Port number used by APs to report location packets. To configure the parameter, run the **11.6.4 aeroscout server** command.
Aeroscout compound-time	Aggregation time of AeroScout location packets. To configure the parameter, run the **11.6.2 aeroscout compound-time** command.

Item	Description
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 the parameter, run the **11.6.4 aeroscout server** command.
Aeroscout via-AC port	Port number used by an AC to report AeroScout location packets. To configure the parameter, run the **11.6.4 aeroscout server** command.
Ekahau-tag	Whether WLAN location of Ekahau tags is enabled. ● enable: The function is enabled. ● disable: The function is disabled. To configure the function, run the **11.6.26 ekahau tag-enable** command.
Ekahau erc IP-address	IP address of the Ekahau location server. To configure the parameter, run the **11.6.25 ekahau server** command.
Ekahau erc port	Port number of the Ekahau location server. To configure the parameter, run the **11.6.25 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 the parameter, run the **11.6.25 ekahau server** command.

Item	Description
Ekahau via-AC port	Port number used by an AC to report Ekahau location packets. To configure the parameter, run the **11.6.25 ekahau server** command.
Source IP-address	Source IP address used by an AC to report location packets. To configure the parameter, run the **11.6.40 source (location profile view)** command.
private mu	Whether terminal location is enabled. ● enable: The function is enabled. ● disable: The function is disabled. To configure the function, run the **11.6.31 private mu-enable** command.
private server	IP address of the terminal location server. To configure the parameter, run the **11.6.33 private server** command.
private server port	Port number of the terminal location server. To configure the parameter, run the **11.6.33 private server** command.
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 the parameter, run the **11.6.33 private server** command.
private via-AC port	Port number used by an AC to report terminal location packets. To configure the parameter, run the **11.6.33 private server** command.
private report-frequency(ms)	Interval at which an AP reports terminal location packets. To configure the parameter, run the **11.6.32 private report-frequency** command.

Item	Description
private mu protocol-version	Terminal location protocol version. To configure the parameter, run the **11.6.30 private mu protocol-version** command.

# Display reference information about the location profile **default**.

```
<HUAWEI> display references location-profile name default
------------------------------------------------------------
Reference type  Reference name                     Reference radio
------------------------------------------------------------
AP group       ap-group1                       Radio-0

AP ID         0                               Radio-1

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

Table 11-145 Description of the **display references location-profile** command output

Item	Description
Reference type	Type of the profile that references the location profile.
Reference name	Name of the profile that references the location profile.
Reference radio	AP radio by which a location profile is referenced

Related Topics

11.6.5 aeroscout tag-enable

11.6.3 aeroscout mu-enable

11.6.4 aeroscout server

11.6.2 aeroscout compound-time

11.6.26 ekahau tag-enable

11.6.25 ekahau server

11.6.31 private mu-enable

11.6.32 private report-frequency

11.6.33 private server

11.6.18 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 **huawei**.

```
<HUAWEI> display references ble-profile name huawei
------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------
AP group                    ap-group1
------------------------------------------------------------------------
Total: 1
```

Table 11-146 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.

11.6.19 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
--------------------------------------------------------------------------------
```

Table 11-147 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.

Related Topics

11.6.8 ble report

11.6.20 display wlan ble monitoring-list

Function

The **display wlan ble monitoring-list** command displays BLE devices that have been added to the 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** command to add BLE devices to the monitoring list, you can run the **display wlan ble monitoring-list** command to check BLE devices that have been added to the monitoring list.

Example

# Check all BLE devices that have been added to the monitoring list.

```
<HUAWEI> display wlan ble monitoring-list
-------------------------------------------------------------------------------
Index       MAC
-------------------------------------------------------------------------------
0          1234-1234-0000
1          1234-1234-7777
-------------------------------------------------------------------------------
Total: 2
```

Table 11-148 Description of the **display wlan ble monitoring-list** command output

Item	Description
Index	Index.
MAC	MAC address of a BLE device that has been added to the monitoring list.

Related Topics

11.6.7 ble monitoring-list

11.6.21 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 **11.6.39 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)
Advertisement data
-------------------------------------------------------------------------------------------------------------------------
0     0000-0101-0202  4           AP4          -30   50%    asset-tag   N           57
02-02-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-fa
1     0000-0101-0303  --          --           -31   51%    asset-tag   N           57
01-02-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-fa
2     0000-0101-0505  12          AP12         -33   55%    asset-tag   N           57
03-02-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-fa
-------------------------------------------------------------------------------------------------------------------------
Total: 3
```

Table 11-149 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.
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.

Related Topics

11.6.39 sniffer enable

11.6.22 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 LBS configuration of the AP with a specified AP ID.	The AP ID must exist.
ap-name *ap-name*	Displays 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 the **display wlan location config-info aeroscout** command to check configurations delivered to APs from the AeroScout location server.

Prerequisites

AeroScout location has been enabled using the **aeroscout tag-enable** or **aeroscout mu-enable** command, and the AeroScout location server has delivered the configuration information to the AP.

Example

# Display AeroScout location configuration on the AP **ap_4**.

```
<HUAWEI> display wlan location config-info aeroscout ap-name ap_4
----------------------------------------------------------------
AP ID                            : 4
AP name                          : ap_4
AP MAC address                   : 1051-7254-5a80
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 11-150 Description of the display wlan location config-info aeroscout command output

Item	Description
AP ID	AP ID.

Item	Description
AP name	Name of the AP.
AP MAC address	MAC address of the AP.
Response IP address	IP address of the location server that receives the Response packets from the AP.
Response port	Listening port of the location server from which the location server receives the Response packets from the AP.
AP tag mode	Tag detection status on the AP: ● start: The AP starts tag detection. ● stop: The AP stops tag detection.
AP MU mode	MU detection status on the AP: ● start: The AP starts tag detection. ● stop: The AP stops tag detection.
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 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 100 milliseconds.

Related Topics

11.6.5 aeroscout tag-enable

11.6.3 aeroscout mu-enable

11.6.23 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       huawei      AeroScout       1040-8002-6f80    11          -50
1       ap3         Ekahau          1040-8002-6420    11          -50
--------------------------------------------------------------------------------
Total: 2
```

Table 11-151 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.

Item	Description
Channel	Working channel of the located tag.
RSSI	RSSI of the located tag, in dBm.

11.6.24 display wlan location statistics aeroscout

Function

The **display wlan location statistics aeroscout** command displays LBS statistics about AeroScout tags and MUs.

Format

display wlan location statistics aeroscout

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

- If APs are configured to report AeroScout tag packets to the AeroScout location server through an AC, the **display wlan location statistics aeroscout** command can display location statistics.
- If APs are configured to report AeroScout tag packets to the AeroScout location server directly but not through an AC, the **display wlan location statistics aeroscout** command cannot display location statistics, and all fields are displayed as "0".

Example

# Displays LBS statistics about AeroScout tags and MUs.

```
<HUAWEI> display wlan location statistics aeroscout
---------------------------------------------------------------
Request protocol version      : 0
Request AP status             : 0
Set configuration             : 0
Set tags mode                 : 0
Set MU mode                   : 0
Request debug information     : 0
ACK                           : 0
NACK                          : 0
```

```
Protocol version report       : 0
AP status report              : 0
Tag report                    : 0
MU report                     : 0
AP debug report               : 0
Compounded reports message    : 0
Generic AP notification       : 0
----------------------------------------------------------------
```

Table 11-152 Description of the display wlan location statistics aeroscout command output

Item	Description
Request protocol version	Number of Request packets that the location server sends to the AP to check the LBS protocol version number supported by the AP.
Request AP status	Number of Request packets that the location server sends to the AP to check support of the AP for the LBS protocol.
Set configuration	Configuration information sent by the location server, which includes multicast MAC address of the tag that the AP needs to detect and the maximum time during which the AP caches tag information.
Set tags mode	Number of packets that the location server sends to the AP to inform the AP to start or stop sending tag information.
Set MU mode	Number of packets that the location server sends to the AP to inform the AP to start or stop sending MU information.
Request debug information	Number of packets that the location server sends to the AP to check AP statistics.
ACK	Number of ACK packets that the AC sends to the location server.
NACK	Number of NACK packets that the AC sends to the location server.
Protocol version report	Number of Response packets sent by the AP to the location server that carry the LBS protocol version number supported by the AP.

Item	Description
AP status report	Number of Response packets sent by the AP to the location server to notify the location server of the radio status and support for the LBS protocol.
Tag report	Number of tag messages sent by the AP.
MU report	Number of MU messages sent by the AP.
AP debug report	Number of packets carrying AP statistics sent by the AP.
Compounded reports message	Number of tag messages that the AP sends to the location server after the cache time set in the **Set configuration** packets expires.
Generic AP notification	Number of packets that the AC sends to the location server to notify the location server of AP errors.

11.6.25 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.
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 configured in the current location profile for a specific location method, it cannot be configured 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 huawei
[HUAWEI-wlan-location-prof-huawei] ekahau server ip-address 192.168.1.2 port 8569
```

Related Topics

11.6.17 display location-profile

11.6.26 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 huawei
[HUAWEI-wlan-location-prof-huawei] ekahau tag-enable
```

11.6.27 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 addresses 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
```

11.6.28 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.
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. Only the AP4030TN, AP4051TN, and AP8050TN-HD supports three radios.
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
```

Related Topics

11.6.17 display location-profile

11.6.29 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

The **location-profile** 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 new 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 **huawei**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name huawei
[HUAWEI-wlan-location-prof-huawei]
```

Related Topics

11.6.17 display location-profile

11.6.30 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 huawei
[HUAWEI-wlan-location-prof-huawei] private mu protocol-version v5
```

Related Topics

11.6.17 display location-profile

11.6.31 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 huawei
[HUAWEI-wlan-location-prof-huawei] private mu-enable
```

11.6.32 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 huawei
[HUAWEI-wlan-location-prof-huawei] private report-frequency 30000
```

Related Topics

11.6.33 private server

11.6.33 private server

Function

The **private server** command configures the destination IP address and port number for APs to report terminal location data.

The **undo private server** command restores the default destination IP address and port number for APs to report terminal location data.

By default, no destination IP address or port number is configured for APs to report terminal location data.

Format

private server ip-address *ip-address* **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 the AP reports terminal location data.	The value is in dotted decimal notation.
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 5000 to 65535.
via-ac	Specifies that terminal location data is sent to a server through an AC	-
ac-port *ac-port-num*	Specifies the destination port number on the AC to which APs report terminal 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 collected 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 terminals 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 terminals, 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 configured in the current location profile for a specific location method, it cannot be configured in other profiles for the same location method.

Example

# Configure APs to report terminal 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 huawei
[HUAWEI-wlan-location-prof-huawei] private server ip-address 192.168.1.2 port 32180
```

Related Topics

11.6.17 display location-profile

11.6.34 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 the **report enable** 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 huawei
[HUAWEI-wlan-ble-prof-huawei] report enable
```

11.6.35 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

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 huawei
[HUAWEI-wlan-ble-prof-huawei] report-mode immediate
```

11.6.36 report-to-server

Function

The **report-to-server** command configures the destination IP address and port number for APs to send Bluetooth packets.

The **undo report-to-server** command restores the default destination IP address and port number for APs to send Bluetooth packets.

By default, no destination IP address or port number is configured for APs to send Bluetooth packets.

Format

report-to-server { **ip-address** *ip-address* | **ipv6-address** *ipv6-address* } **port** *port-num* [**via-ac ac-port** *ac-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 send Bluetooth packets.	The value is in dotted decimal notation.
ipv6-address *ipv6-address*	Specifies the IPv6 address of the location server to which APs send Bluetooth packets.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
port *port-num*	Specifies the destination port number on the location server to which APs directly report Bluetooth packets. Specifies the destination port number on the location server to which APs report Bluetooth packets through an AC.	The value is an integer that ranges from 5000 to 65535.
via-ac	Specifies that Bluetooth packets are sent to a server through an AC.	-
ac-port *ac-port-num*	Specifies the destination 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:

- Report the data directly to a server.
- Report the data to a 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 forwarding through an AC can be configured only in one BLE profile. If Bluetooth data forwarding 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 send 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 huawei
[HUAWEI-wlan-ble-prof-huawei] report-to-server ip-address 192.168.1.2 port 8569
```

11.6.37 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 BEL devices from the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] reset wlan ble site-info all
```

11.6.38 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
```

Related Topics

11.6.23 display wlan location device-info tag

11.6.39 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 configured working mode 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 enabling the Bluetooth monitoring or Bluetooth tag location function, the built-in Bluetooth module of an AP will scan and obtain information about surrounding BLE devices or Bluetooth tags, and 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 time (for example, 2:00 am of the 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.

The Bluetooth broadcast and Bluetooth monitoring functions can be enabled simultaneously for an AP's built-in Bluetooth module. When the two functions are enabled simultaneously, 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 huawei
[HUAWEI-wlan-ble-prof-huawei] sniffer enable ibeacon-mode
Warning: Modifying the monitoring mode may cause BLE devices in the original monitoring mode to go offline and age.
```

Related Topics

11.6.7 ble monitoring-list

11.6.16 display ble-profile

11.6.21 display wlan ble site-info

11.6.40 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 addresses 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 huawei
[HUAWEI-wlan-location-prof-huawei] source ip-address 10.102.25.23
```

11.6.41 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 **11.6.41 source (BLE profile view)** and **11.6.9 ble source** commands are both executed, the function configured using the **11.6.41 source (BLE profile view)** command takes effect.

Example

# Configure the source IP address of the 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 huawei
[HUAWEI-wlan-ble-prof-huawei] source ip-address 10.102.25.23
```

Related Topics

11.6.9 ble source

11.6.42 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.

By default, the 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	Transmit power of an AP's built-in Bluetooth module.	The value is an 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 transmit power can improve Bluetooth signal transmission quality but causes more severe interference to other wireless devices.

Reducing transmit power can reduce interference to other wireless devices but affects Bluetooth signal transmission quality. Configure proper transmit power of an AP's built-in Bluetooth module according to actual situations.

Precautions

After changing the transmit power of an AP's built-in Bluetooth module, you need to run the **11.6.13 broadcasting-content** command to reconfigure the RSSI calibration value in BLE broadcast frames.

Example

# Configure 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 huawei
[HUAWEI-wlan-ble-prof-huawei] tx-power 2
```

Related Topics

11.6.13 broadcasting-content

11.6.16 display ble-profile

11.7 WLAN Security Configuration Commands

11.7.1 Command Support

Only the S5720HI supports WLAN-AC commands.

11.7.2 anti-attack broadcast-flood blacklist enable

Function

The **anti-attack broadcast-flood blacklist enable** command enables the broadcast flood blacklist function.

The **undo anti-attack broadcast-flood blacklist enable** command disables the broadcast flood blacklist function.

By default, the broadcast flood blacklist function is disabled.

Format

anti-attack broadcast-flood blacklist enable

undo anti-attack broadcast-flood blacklist enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the broadcast flood blacklist function is enabled, the device considers traffic with a rate higher than that specified in **11.7.4 anti-attack broadcast-flood sta-rate-threshold** a broadcast flood attack and adds the STA to the blacklist.

Prerequisites

The broadcast flood detection function has been enabled using the **undo** **11.7.3 anti-attack broadcast-flood disable** command.

Example

# Enable the broadcast flood blacklist function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name profile1
[HUAWEI-wlan-vap-prof-profile1] anti-attack broadcast-flood blacklist enable
```

Related Topics

11.7.3 anti-attack broadcast-flood disable

11.7.4 anti-attack broadcast-flood sta-rate-threshold

11.7.3 anti-attack broadcast-flood disable

Function

The **anti-attack broadcast-flood disable** command disables the broadcast flood detection function.

The **undo anti-attack broadcast-flood disable** command enables the broadcast flood detection function.

By default, the broadcast flood detection function is enabled.

Format

anti-attack broadcast-flood disable

undo anti-attack broadcast-flood disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a large number of broadcast packets are sent to a device in a short time, the device becomes busy processing the packets and cannot process normal services. To prevent broadcast flood attacks, you can configure broadcast flood detection.

Example

# Disable the broadcast flood detection function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name profile1
[HUAWEI-vap-prof-profile1] anti-attack broadcast-flood disable
```

Related Topics

11.7.4 anti-attack broadcast-flood sta-rate-threshold

11.7.4 anti-attack broadcast-flood sta-rate-threshold

Function

The **anti-attack broadcast-flood sta-rate-threshold** command sets the broadcast flood threshold.

The **undo anti-attack broadcast-flood sta-rate-threshold** command restores the default broadcast flood threshold.

By default, the broadcast flood threshold is 10 pps.

Format

anti-attack broadcast-flood sta-rate-threshold *sta-rate-threshold*

undo anti-attack broadcast-flood sta-rate-threshold

Parameters

Parameter	Description	Value
sta-rate-threshold	Specifies the rate threshold of broadcast traffic from STAs.	The value is an integer that ranges from 5 to 5000, in pps.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the broadcast flood detection function is enabled, you can set the broadcast traffic threshold.

When the traffic rate exceeds the threshold, the device considers a broadcast flood attack from the STA and discards the broadcast traffic. This prevents the upper-layer network from being affected by the broadcast flood.

If the broadcast flood blacklist function is enabled using the **11.7.2 anti-attack broadcast-flood blacklist enable** command, the device adds broadcast flood STAs to the blacklist.

Prerequisites

The broadcast flood detection function has been enabled using the **undo 11.7.3 anti-attack broadcast-flood disable** command.

Example

# Set the broadcast flood threshold to 100 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name profile1
[HUAWEI-vap-prof-profile1] anti-attack broadcast-flood sta-rate-threshold 100
```

Related Topics

11.7.3 anti-attack broadcast-flood disable

11.7.2 anti-attack broadcast-flood blacklist enable

11.7.5 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
```

Related Topics

11.1.152 display vap-profile

11.7.6 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 **11.7.38 dynamic-blacklist enable** 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 office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids attack detect enable wpa-psk
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name huawei
[HUAWEI-wlan-wids-prof-huawei] brute-force-detect interval 100
```

Related Topics

11.7.79 wids attack detect enable

11.7.8 brute-force-detect threshold

11.7.38 dynamic-blacklist enable

11.7.7 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 time, 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 avoid frequent alarm reports.

Follow-up Procedure

Run the **11.7.38 dynamic-blacklist enable** 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 office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids attack detect enable wpa-psk
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name huawei
[HUAWEI-wlan-wids-prof-huawei] brute-force-detect quiet-time 300
```

Related Topics

11.7.79 wids attack detect enable

11.7.38 dynamic-blacklist enable

11.7.8 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 **11.7.38 dynamic-blacklist enable** 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 office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids attack detect enable wpa-psk
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name huawei
[HUAWEI-wlan-wids-prof-huawei] brute-force-detect threshold 60
```

Related Topics

11.7.79 wids attack detect enable

11.7.38 dynamic-blacklist enable

11.7.9 contain-mode

Function

The **contain-mode** command sets the containment mode against rogue devices.

The **undo contain-mode** command deletes the containment mode against rogue devices.

By default, no containment mode against rogue 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 APs.	-
spoof-ssid-ap	Sets the containment mode against rogue APs using spoofing SSIDs.	-
client	Sets the containment mode against unauthorized 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 APs.	-
adhoc	Sets the containment mode against Ad-hoc devices.	-

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Rogue devices pose serious security threats to enterprise networks.

After the containment mode is set against rogue APs, the monitor AP uses the identity of the rogue AP to broadcast deauthentication frames to forcibly disconnect STAs. To prevent the STAs from connecting to the rogue AP again, the monitor AP will periodically and continuously send deauthentication frames.

After the containment mode is set against rogue 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 APs with spoofing SSIDs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids contain enable
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name huawei
[HUAWEI-wlan-wids-prof-huawei] contain-mode spoof-ssid-ap
```

Related Topics

11.7.80 wids contain enable

11.7.10 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 10 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 clear 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 office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids device detect enable
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name office
[HUAWEI-wlan-wids-prof-office] device report-interval 120
```

Related Topics

11.7.81 wids device detect enable

11.7.11 device synchronization-interval

Function

The **device synchronization-interval** command sets the interval at which an AP reports all wireless device information.

The **undo device synchronization-interval** command restores the default interval at which an AP reports all wireless device information.

By default, an AP reports all wireless device information to an AC at an interval of 360 minutes.

Format

device synchronization-interval *interval*

undo device synchronization-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an AP reports all wireless device information.	The value is an integer that ranges from 120 to 360, in minutes.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP reports wireless device information in the following modes:

- Incremental reporting: The AP reports the added, changed, or deleted information to the AC in real time.
- All information reporting: The AP periodically reports all wireless device information to the AC.

To ensure that detected device information is consistent on the AP and AC, run the **device synchronization-interval** command to enable the AP to periodically synchronize wireless device information to the AC.

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 all wireless device information to 120 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids device detect enable
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name office
[HUAWEI-wlan-wids-prof-office] device synchronization-interval 120
```

Related Topics

11.7.81 wids device detect enable

11.7.12 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 disabled in the VAP profile view and 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

VAP profile view, AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a bogus DHCP server is deployed at the user side, STAs may obtain incorrect IP addresses and network configuration parameters and cannot communicate properly. After the **undo dhcp trust port** command is executed in the VAP profile view, an AP discards the DHCP OFFER, ACK, and NAK packets sent by the bogus DHCP server and reports to the AC about the IP address of the unauthorized DHCP server.

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 the 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 **11.1.179 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 the VAP profile **vap1** and configure a DHCP 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] dhcp trust port
```

Related Topics

11.1.152 display vap-profile

11.1.120 display ap-system-profile

11.7.13 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 you run this command. Continue?
[Y/N]y
Info: This operation may take a few seconds. Please wait for a moment.done.
p:            permit
i:           interference
Ch:           Channel
NF:           Noise Floor
CommIf:       Common-Channel Interference
AdjaceIf:     Adjacent-Channel Interference
#AP:          Number of APs detected
Radio:        0
ScanChannel:  1
WorkChannel:  1
ScanCycle:    1
--------------------------------------------------------------------------
Ch  NF   CU(%) CommIf(%) AdjaceIf(%) SINR  #APs
--------------------------------------------------------------------------
1   -105 75    19        -           245       57
--------------------------------------------------------------------------
Total: 1
--------------------------------------------------------------------------
Ch    MAC            Type  RSSI  SSID
--------------------------------------------------------------------------
1     c88d-833a-8d41 i     -65   xw9-2g-tunnel
-----------------------------------------------
Total: 1
```

Table 11-153 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.
#APs	Number of scanned APs.

Item	Description
SINR	Signal to interference plus noise ratio (SINR).
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 channel utilization (higher than 80%) or 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.

11.7.14 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 **huawei**.

```
<HUAWEI> display references wids-whitelist-profile name huawei
------------------------------------------------------------
Profile type                Reference name
------------------------------------------------------------
wids-profile                 huawei
------------------------------------------------------------
Total: 1
```

Table 11-154 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.

11.7.15 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 **huawei**.

```
<HUAWEI> display references wids-profile name huawei
------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------
AP group                   default
AP ID                      0
------------------------------------------------------------------------
Total: 2
```

Table 11-155 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.

11.7.16 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 **huawei**.

```
<HUAWEI> display references wids-spoof-profile name huawei
Profile type                  Reference name
--------------------------------------------------------------
wids-profile                  huawei
--------------------------------------------------------------
Total: 1
```

Table 11-156 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.

11.7.17 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
------------------------------------------------------------
huawei                            0
office                          0
office1                          1
------------------------------------------------------------
Total: 3
```

Table 11-157 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 **huawei**.

```
<HUAWEI> display wids-whitelist-profile name huawei
------------------------------------------------------------
Type          Content
```

```
------------------------------------------------------------
MAC          0011-2233-4455
OUI         00-11-22
SSID        huawei
------------------------------------------------------------
Total: 3
```

Table 11-158 Description of the **display wids-whitelist-profile name** command output

Item	Description
Type	Type of authorized APs.
Content	Rule for authorized APs. To set the rule, run the **11.7.46 permit-ap** command.

Related Topics

11.7.46 permit-ap

11.7.18 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                          3
huawei                            2
office                          0
office01                         0
------------------------------------------------------------
Total: 4
```

Table 11-159 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 **huawei**.

```
<HUAWEI> display wids-profile name huawei
------------------------------------------------------------
Device report interval(s)           : 10
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
                               Ad hoc
STA whitelist profile               :
WIDS spoof profile                  : huawei
WIDS whitelist profile              : huawei
------------------------------------------------------------
```

Table 11-160 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 set the interval, run the **11.7.10 device report-interval** command.
Brute force detect interval(s)	Interval for brute force key cracking detection. To set the interval, run the **11.7.6 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 set the maximum number, run the **11.7.8 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 set the quiet time, run the **11.7.7 brute-force-detect quiet-time** command.
Flood detect interval(s)	Flood attack detection interval. To set the interval, run the **11.7.39 flood-detect interval** command.
Flood detect threshold	Flood attack detection threshold. To set the threshold, run the **11.7.41 flood-detect threshold** command.
Flood quiet time(s)	Quiet time for an AP to report the detected flood attacks to the AC. To set the quiet time, run the **11.7.40 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 set the quiet time, run the **11.7.76 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 set the quiet time, run the **11.7.60 spoof-detect quiet-time** command.

Item	Description
Dynamic blacklist	Whether the dynamic blacklist function is enabled. To configure the function, run the **11.7.38 dynamic-blacklist enable** command.
Contain rogue mode	Countering mode against rogue devices. To set the countering mode, run the **11.7.9 contain-mode** command.
STA whitelist profile	STA protection based on a STA whitelist. To set the countering mode, run the **11.7.9 contain-mode** command.
WIDS spoof profile	WIDS spoof profile bound to the WIDS profile. To bind a WIDS spoof profile to a WIDS profile, run the **11.7.87 wids-spoof-profile (WIDS profile view)** command.
WIDS whitelist profile	WIDS whitelist profile bound to the WIDS profile. To bind a WIDS whitelist profile to a WIDS profile, run the **11.7.83 wids-whitelist-profile (WIDS profile view)** command.

Related Topics

11.7.10 device report-interval

11.7.6 brute-force-detect interval

11.7.8 brute-force-detect threshold

11.7.7 brute-force-detect quiet-time

11.7.39 flood-detect interval

11.7.41 flood-detect threshold

11.7.40 flood-detect quiet-time

11.7.76 weak-iv-detect quiet-time

11.7.60 spoof-detect quiet-time

11.7.38 dynamic-blacklist enable

11.7.9 contain-mode

11.7.87 wids-spoof-profile (WIDS profile view)

11.7.83 wids-whitelist-profile (WIDS profile view)

11.7.19 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
------------------------------------------------------------
huawei                   0
office1                 1
------------------------------------------------------------
Total: 2
```

Table 11-161 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 **huawei**.

```
<HUAWEI> display wids-spoof-profile name huawei
------------------------------------------------------------
ID      Pattern rule
------------------------------------------------------------
0       ^HUAWE[1l]$
------------------------------------------------------------
Total: 1
```

Table 11-162 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 **11.7.61 spoof-ssid** command.

Related Topics

11.7.61 spoof-ssid

11.7.20 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 11-163 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.

11.7.21 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 11-164 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.

11.7.22 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 11-165 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.

11.7.23 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 configurations of all security profiles.

```
<HUAWEI> display security-profile all
---------------------------------------------------------
Profile name                    Reference
---------------------------------------------------------
default                      1
default-wds                    1
default-mesh                    1
security-profile1              0
---------------------------------------------------------
Total: 3
```

Table 11-166 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    : -
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 11-167 Description of the **display security-profile name** command output

Item	Description
Security policy	Security policy. The following security policies are supported: ● Open system: open system authentication ● Share key: WEP Shared Key ● WPA 802.1X ● WPA2 802.1X ● WPA-WPA2 802.1X ● WPA PSK: WPA Pre-Shared Key ● WPA2 PSK: WPA2 Pre-Shared Key ● WPA-WPA2 PSK: WPA-WPA2 Pre-Shared Key ● WAPI PSK: WAPI Pre-Shared Key ● WAPI certificate To configure the parameter, run the **11.7.57 security wep**, **11.7.54 security dot1x**, **11.7.55 security psk** and **11.7.56 security wapi** commands.

Item	Description
Encryption	Encryption mode. The following encryption modes are supported: TKIP, AES, AES-TKIP, WEP-40, WEP-104, WEP-128, and SMS4. WAPI encryption uses SMS4. To configure the parameter, run the **11.7.78 wep key**, **11.7.54 security dot1x** and **11.7.55 security psk** commands.
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. To configure this function, run the **11.7.47 pmf** command.
Key *key-id*	Key ID. To configure the parameter, run the **11.7.78 wep key** command.
Default key ID	Default key ID. To configure the parameter, run the **11.7.77 wep default-key** command.
PTK update	Whether to enable periodic PTK update in WPA, WPA2 or WPA-WPA2 authentication and encryption. ● enable: Enables periodic PTK update. ● disable: Disables periodic PTK update. To configure the parameter, run the **11.7.89 wpa ptk-update enable** command.

Item	Description
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 the parameter, run the **11.7.90 wpa ptk-update ptk-update-interval** command.
CA certificate filename	CA certificate file name. To configure the parameter, run the **11.7.69 wapi import certificate** command.
ASU certificate filename	File name of the authentication server unit (ASU) certificate. To configure the parameter, run the **11.7.69 wapi import certificate** command.
AC certificate filename	AC certificate file name. To configure the parameter, run the **11.7.69 wapi import certificate** command.
AC private key filename	AC private key file name. To configure the parameter, run the **11.7.70 wapi import private-key** command.
WAPI source interface	WAPI source interface. To configure the parameter, run the **11.7.74 wapi source interface** command.
Authentication server IP	IP address of the ASU certificate server. To configure the parameter, run the **11.7.66 wapi asu** command.
WAI timeout(s)	Timeout period of an association. To configure the parameter, run the **11.7.73 wapi sa-timeout** command.
BK update interval(s)	Interval for updating the base key (BK). To configure the parameter, run the **11.7.67 wapi bk** command.
BK lifetime threshold(%)	Threshold for triggering BK update. To configure the parameter, run the **11.7.67 wapi bk** command.

Item	Description
USK update method	Whether the USK is updated based on a time interval or a packet count. To configure the parameter, run the **11.7.71 wapi key-update** command.
USK update interval(s)	Time-based interval for updating the unicast session key (USK). To configure the parameter, run the **11.7.75 wapi usk** command.
MSK update method	Whether the MSK is updated based on a time interval or a packet count. To configure the parameter, run the **11.7.71 wapi key-update** command.
MSK update interval(s)	Time-based interval for updating the MBMS service key (MSK). To configure the parameter, run the **11.7.72 wapi msk** command.
Cert auth retrans count	Number of retransmissions of certificate authentication packets. To configure the parameter, run the **11.7.68 wapi cert-retrans-count** command.
USK negotiate retrans count	Number of retransmissions of USK negotiation packets. To configure the parameter, run the **11.7.75 wapi usk** command.
MSK negotiate retrans count	Number of retransmissions of MSK negotiation packets. To configure the parameter, run the **11.7.72 wapi msk** command.

11.7.24 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 for VAPs, 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 11-168 Description of the **display sta-blacklist-profile all** command output

Item	Description
Profile name	Name of a STA blacklist profile.
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          0021-1111-2222
------------------------------------------------------------
Total: 1
```

Table 11-169 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 **11.7.64 sta-mac** command.
Description	Adds MAC address description to a blacklist.

Related Topics

11.7.64 sta-mac

11.7.25 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.
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. The aging time of the dynamic blacklist entries is 10 minutes. After the aging time is reached, the dynamic blacklist entries are 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 huawei
Total: 1
----------------------------------------------------------------------------
STA MAC          Time left(s)   Reason
----------------------------------------------------------------------------
581f-28fc-7ead    160          static ip
----------------------------------------------------------------------------
```

Table 11-170 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 **11.7.37 dynamic-blacklist aging-time** command.
Reason	STA access denial reason. ● static ip: The AP is configured to deny access of STAs with bogus IP addresses, and the STA has a static IP address configured. ● broadcast flood: The AP is configured to detect and defend against broadcast flood attacks, and the STA initiates a broadcast flood attack. ● **WIDS attack**: The AP is configured to detect attacks on a WLAN. ● **MESH key fail**: Key negotiation fails during mesh link setup.

Related Topics

11.7.37 dynamic-blacklist aging-time

11.7.26 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 11-171 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         0021-1111-2222
------------------------------------------------------------
Total: 1
------------------------------------------------------------
Index      OUI                 Description
------------------------------------------------------------
0         00-00-01
------------------------------------------------------------
Total: 1
```

Table 11-172 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 **11.7.64 sta-mac** command.
OUI	OUI of a STA in the whitelist. To configure the parameter, run the **11.7.45 oui** command.
Description	Adds MAC address description to a whitelist.

Related Topics

11.7.64 sta-mac

11.7.27 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 the **display wlan ids attack-detected** command to view information about the attacking devices.

Prerequisites

The attack detection functions of all types have been enabled using the **11.7.79 wids attack detect enable** command.

Example

# Display information of 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
-------------------------------------------------------------------------------
000b-c002-9c81  pbr    165  -87        2014-11-20/15:51:13    1
0024-2376-03e9  pbr    165  -84        2014-11-20/15:52:13    1
0046-4b74-691f  act    165  -67        2014-11-20/15:43:33    1
00bc-71b7-171d  pbr    165  -88        2014-11-20/15:41:43    1
00bc-71b7-171f  act    165  -87        2014-11-20/15:44:03    1
-------------------------------------------------------------------------------
Total: 5, printed: 5
```

Table 11-173 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 is detected.

Item	Description
#AP	Number of APs which detect this attack.

# Display information of an attacking device with the specified MAC address.

```
<HUAWEI> display wlan ids attack-detected mac-address 8c70-5a47-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                          : 8c70-5a47-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 11-174 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.

Related Topics

11.7.79 wids attack detect enable

11.7.28 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 **11.7.79 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 11-175 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.

Related Topics

11.7.79 wids attack detect enable

11.7.29 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 of the detected attacking device 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 **11.7.79 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
--------------------------------------------------------------------------------
2477-039a-37ec  pbr   165  -86        2014-11-20/15:51:43   ap-13
00bc-71b7-171d  pbr   165  -88        2014-11-20/15:41:43   ap-13
2477-039a-0bf4  pbr   165  -81        2014-11-20/15:41:53   ap-13
--------------------------------------------------------------------------------
Total: 3, printed: 3
```

Table 11-176 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 attack type.

Item	Description
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.

Related Topics

11.7.79 wids attack detect enable

11.7.30 display wlan ids contain

Function

The **display wlan ids contain** command displays information about countered 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-id** *radio-id*] }

Parameters

Parameter	Description	Value
all	Displays information about all countered devices.	-
ap	Displays information about countered APs.	-
adhoc	Displays information about countered Adhoc devices.	-
client	Displays information about countered user terminals.	-
ssid	Displays information about countered devices with unauthorized SSIDs.	-
mac-address *mac-address*	Displays information about countered devices with specified MAC addresses.	The MAC addresses must exist.

Parameter	Description	Value
monitor-ap ap-name *ap-name*	Displays information about countered 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 countered 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-id** *radio-id*	Displays information about countered 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 the **display wlan ids countermeasures device** command to view information about countered devices.

Example

# Display the list of all countered 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   SSID
--------------------------------------------------------------------------------
88e3-abbf-b93d   11  open             2014-11-20/16:16:57  1     -
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-177 Description of the **display wlan ids contain all** command output

Item	Description
MAC address	MAC address of the countered device.
CH	Channel in which the monitoring AP detects a device for the last time.

Item	Description
Authentication	Authentication mode of the countered device.
Last detected time	Last time at which the monitoring AP detects a device.
#Rf	Number of monitor radios that have contained the device.
SSID	SSID of the countered device.

# Display information about countered 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 11-178 Description of the **display wlan ids contain ssid** command output

Item	Description
SSID	Countered SSID.
#Dev	Number of devices that use the SSID.
Last detected time	Last time at which the device using the SSID is detected.

# Display information about countered devices with specified MAC addresses.

```
<HUAWEI> display wlan ids contain mac-address 549f-13c4-627f
-------------------------------------------------------------------------------
MAC address                                        : 549f-13c4-627f
BSSID                                              : dcd2-fc9a-c808
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(ms)                                : 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                                       : dcd2-fc1e-c4a0
 Radio type                                        : 802.11bg
 Channel                                           : 1
 RSSI(dBm)                                         : -54
 Last detected time                                : 2015-10-20/15:06:26
```

```
Counter measure                                     : Y
--------------------------------------------------------------------------------
```

Table 11-179 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.
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 in which the device is detected for the last time.
Maximum RSSI(dBm)	Maximum RSSI of the detected device.
Beacon interval(ms)	Interval at which the detected device sends Beacon frames.
First detected time	First time at which the device is detected.
Reported AP 1	Information of the Monitoring AP which reports detection information.
AP name	Name of the monitoring AP.
Radio ID	Radio ID of the monitoring AP.
MAC address	MAC address of the monitoring AP.
Radio type	Radio type of the monitoring AP.
Channel	Channel of the monitoring AP.
RSSI(dBm)	RSSI of the monitoring AP.
Last detected time	Last time when the device is detected.
Counter measure	Whether the device is contained.

# Display the list of countered devices among the wireless devices detected by the monitoring AP **huawei**.

```
<HUAWEI> display wlan ids contain monitor-ap ap-name huawei
Countermeasures Device Profile
------------------------------------------------------------------------------
AP MAC address                            : dcd2-fc1e-c4a0
AP type                                   : AP6010DN-AGN
AP name                                   : huawei
Contain device 0
  MAC address                             : c46a-b7bc-7b83
  BSSID                                   : 0006-f476-e210
  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
------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-180 Description of the **display wlan ids contain monitor-ap** command output

Item	Description
AP MAC address	MAC address of the monitoring AP.
AP type	Type of the monitoring AP.
AP name	Name of the monitoring AP.
MAC address	MAC address of the countered device.
BSSID	BSSID of the countered device.
Type	Type of the countered device.
SSID	SSID of the countered device.
Authentication	Authentication mode of the countered device.
Last detected channel by this AP	Channel in which the monitoring AP detects a countered device for the last time.
Maximum RSSI(dBm)	Maximum RSSI of the countered device.
Beacon interval(TUs)	Interval at which the countered device sends Beacon frames.
First detected time	First time at which the device is detected.

11.7.31 display wlan ids device-detected

Function

The **display wlan ids device-detected** command displays various wireless devices detected on a WLAN.

Format

display wlan ids device-detected { **all** | [**interference** | **rogue**] **ap** | [**rogue**] **bridge** | [**rogue**] **client** | **adhoc** | [**rogue**] **ssid** | **mac-address** *mac-address* | **monitor-ap** { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio-id** *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.	-
adhoc	Displays detected user terminals that belong to the Ad-hoc network on the WLAN.	-
ssid	Displays SSIDs detected on the WLAN.	-
mac-address *mac-address*	Displays detailed information about devices with specified MAC addresses detected on the WLAN.	The MAC addresses must exist.
monitor-ap ap-name *ap-name*	Displays detailed information about devices detected by the monitoring 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 monitoring 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-id** *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 **11.7.81 wids device detect enable** command.

Example

# Display all devices detected on a 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
------------------------------------------------------------------------------
MAC address     Type    CH  Authentication   Last detected time   #Rf   SSID
------------------------------------------------------------------------------
0010-0020-de2b  r/i/w   1   open            2014-11-20/11:03:44  1     -
------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-181 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
Authentication	Authentication mode of the detected device.
CH	Channel in which the device is detected for the last time.
Last detected time	Last time when the device is 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
-------------------------------------------------------------------------------
MAC address     Type  CH  Authentication   Last detected time   #Rf   SSID
-------------------------------------------------------------------------------
0010-0020-de2b  r/i   1   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
-------------------------------------------------------------------------------
MAC Address     CH  Authentication   Last detected time   #Rf   SSID
-------------------------------------------------------------------------------
0010-0020-de2b  1   open            2014-11-20/11:03:44  1     -
-------------------------------------------------------------------------------
Total: 1, printed: 1
```

# Display information about interfering APs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected interference ap
Flags: r: rogue, p: permit
#Rf: Number of monitor radios that have detected the device
CH: Channel number
-------------------------------------------------------------------------------
MAC address     Type  CH  Authentication   Last detected time   #Rf   SSID
```

```
--------------------------------------------------------------------------------
0010-0020-de2b  r     1   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
--------------------------------------------------------------------------------
MAC address     Type  CH  Authentication   Last detected time   #Rf   SSID
--------------------------------------------------------------------------------
0010-0020-de2d  r     6   open           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 11-182 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 is 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 11-183 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	Latest time when the SSID is detected.

# Display detailed information about devices with MAC address 587f-66d4-d569 detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected mac-address 587f-66d4-d569
Detected MAC List
--------------------------------------------------------------------------------
MAC address                              : 587f-66d4-d569
BSSID                                  : 0008-cbe9-1c00
Type                                  : rogue client
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                             : dcd2-fc1e-c4a0
 Radio type                             : 802.11bg
 Channel                               : 1
 RSSI(dBm)                              : -80
 Last detected time                       : 2015-10-20/15:07:23
 Counter measure                          : Y
--------------------------------------------------------------------------------
```

Table 11-184 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.

Item	Description
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 is detected.
Reported AP 1	Information of the Monitoring AP which reports detection information.
AP name	Name of the monitoring AP.
Radio ID	Radio ID of the monitoring AP.
MAC address	MAC address of the monitoring AP.
Radio type	Radio type of the monitoring AP.
Channel	Channel of the monitoring AP.
RSSI(dBm)	RSSI of the monitoring AP.
Last detected time	Last time when the device is detected.
Counter measure	Whether the devices is contained.

11.7.32 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 11-185 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.

Item	Description
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.

11.7.33 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 a specified AP.	The AP ID must exist.
ap-name *ap-name*	Displays information about attacking devices detected by a specified AP.	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 the **display wlan dynamic-blacklist** command to view information about devices in the dynamic blacklist.

Prerequisites

- The dynamic blacklist function has been enabled using the **11.7.38 dynamic-blacklist enable** command.
- The attack detection functions of all types have been enabled using the **11.7.79 wids attack detect enable** command.

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
-------------------------------------------------------------------------------
0006-f476-cb70    2015-07-27/12:51:25   brf       1    100
0006-f476-ce90    2015-07-27/12:51:25   pbr       1    200
0006-f476-d35d    2015-07-27/12:51:25   pbr       1    200
0006-f476-d910    2015-07-27/12:51:25   sti       1    200
0006-f476-dd30    2015-07-27/12:51:25   pbr       1    200
0006-f476-df30    2015-07-27/12:51:25   pbr       1    200
-------------------------------------------------------------------------------
Total: 6, printed: 6
```

Table 11-186 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.

Item	Description
Reason	Reason why the device is added to the dynamic blacklist. The values here are the acronyms of attack types. For details, see **11.7.27 display wlan ids attack-detected**.
#AP	Number of APs that have detected and added the device to the dynamic blacklist.
LAT	Left 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
-------------------------------------------------------------------------------
0006-f476-cb70    2015-07-27/12:51:25    sti      100
0006-f476-ce90    2015-07-27/12:51:25    brf      200
0006-f476-ced0    2015-07-27/12:51:30    pbr      200
0006-f476-d35d    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 0006-f476-cb70
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 11-187 Description of the **display wlan dynamic-blacklist mac-address** command output

Item	Description
AP name	Name of the monitor AP.

Item	Description
Last detected time	Latest time when the device was detected.
Reason	Reason why the device is added to the dynamic blacklist.
LAT	Left aging time for the device in the dynamic blacklist.
BT	Duration for which the device is in the dynamic blacklist.

Related Topics

11.7.38 dynamic-blacklist enable

11.7.79 wids attack detect enable

11.7.34 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.	-
bridge	Displays historical records of rogue bridge devices.	-
client	Displays historical records of rogue user terminals.	-
adhoc	Displays historical records of rogue Adhoc devices.	-
ssid	Displays historical records of countered devices with unauthorized SSIDs.	-

Parameter	Description	Value
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 **11.7.81 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
-------------------------------------------------------------------------------
000a-f7bc-1852  w     11  open             2014-11-20/11:20:37  wlan
000b-c002-9c81  c     11  -                2014-11-20/11:16:07  -
-------------------------------------------------------------------------------
Total: 2, printed: 2
```

Table 11-188 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.

Item	Description
Type	Type of the rogue device listed in the historical record list: ● a: user terminal on the Adhoc 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
--------------------------------------------------------------------------------
000a-f7bc-1852  11  open             2014-11-20/11:20:37  wlan
0022-aad0-c672  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 11-189 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.

Item	Description
Last detected time	Last time at which the device using the SSID is detected.

# Display historical records of an AP or client 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 11-190 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 extended service set (ESS).
Authentication	Authentication mode of the detected device.
Last detected time	Last time when the device is detected.

11.7.35 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  huawei
HUAWEl                             1    2014-03-06/12:44:50  huawei
-------------------------------------------------------------------------------
Total: 2
```

Table 11-191 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.

Related Topics

11.7.61 spoof-ssid

11.7.36 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 visible 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 11-192 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	Algorithm used to calculate the signature.
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.

11.7.37 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 600 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 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name huawei
[HUAWEI-wlan-ap-system-prof-huawei] dynamic-blacklist aging-time 300
```

Related Topics

11.7.38 dynamic-blacklist enable

11.7.38 dynamic-blacklist enable

Function

The **dynamic-blacklist enable** command enables the dynamic blacklist function.

The **undo dynamic-blacklist enable** command disables the dynamic blacklist function.

By default, the dynamic blacklist function is disabled.

Format

dynamic-blacklist enable

undo dynamic-blacklist enable

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 **dynamic-blacklist enable** 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 discard 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 **11.7.37 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 huawei
[HUAWEI-wlan-wids-prof-huawei] dynamic-blacklist enable
```

Related Topics

11.7.37 dynamic-blacklist aging-time

11.7.39 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 **11.7.38 dynamic-blacklist enable** 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 office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids attack detect enable flood
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name huawei
[HUAWEI-wlan-wids-prof-huawei] flood-detect interval 120
```

Related Topics

11.7.79 wids attack detect enable

11.7.38 dynamic-blacklist enable

11.7.40 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 **11.7.38 dynamic-blacklist enable** 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 office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids attack detect enable flood
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name huawei
[HUAWEI-wlan-wids-prof-huawei] flood-detect quiet-time 300
```

Related Topics

11.7.79 wids attack detect enable

11.7.38 dynamic-blacklist enable

11.7.41 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 **11.7.38 dynamic-blacklist enable** 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 office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids attack detect enable flood
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name huawei
[HUAWEI-wlan-wids-prof-huawei] flood-detect threshold 350
```

Related Topics

11.7.79 wids attack detect enable

11.7.38 dynamic-blacklist enable

11.7.42 ip source check user-bind enable

Function

The **ip source check user-bind enable** command enables IP source guard on APs.

The **undo ip source check user-bind enable** command disables IP source guard on APs.

By default, IP source guard 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 IP source guard on APs.

To prevent IP packets of unauthorized users from entering external networks through an AP, enable IP source guard in a VAP profile and bind the VAP profile to an AP or AP group. The IP source guard function can filter incoming packets on an AP radio interface, preventing unauthorized packets from passing through the AP.

If STA address learning is enabled on an AP using the **undo learn-client-address disable** command, DHCP users are allowed to access the AP. Before the users who are assigned IP addresses statically access an AP, the administrator needs to manually configure static binding entries for the users. That is, the administrator configures an IP network segment and binds it to the MAC addresses of the users so that the users can access the AP.

Example

# Enable IP source guard 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
```

Related Topics

11.1.152 display vap-profile

11.7.25 display station dynamic-blacklist

11.7.44 learn-client-address disable (VAP profile view)

11.7.43 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

The DHCP trusted port has been disabled using the **undo dhcp trust port** command in the VAP profile view.

STA address learning has been enabled using the **undo learn-client-address disable** command.

Precautions

After strict STA IP address learning is enabled, it is recommended that you run the **11.7.42 ip source check user-bind enable** and **11.7.5 arp anti-attack check user-bind enable** commands to enable IP source guard and dynamic ARP inspection so that STAs cannot communicate with the network before obtaining an IP address through DHCP.

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
```

Related Topics

11.7.5 arp anti-attack check user-bind enable

11.1.152 display vap-profile

11.7.42 ip source check user-bind enable

11.7.44 learn-client-address disable (VAP profile view)

Function

learn-client-address disable command disables STA IPv4 address learning.

undo learn-client-address disable command disables STA IPv4 address learning.

By default, STA address learning is enabled.

Format

learn-client-address ipv4 disable

undo learn-client-address ipv4 disable

Parameters

Parameter	Description
ipv4	

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a STA associates with an AP that has STA address learning enabled and obtains an IP address, the AP automatically reports the STA IP address to the AC to maintain the STA' IP address and MAC address binding entry

Prerequisites

- Before disabling STA address learning, run the **undo dhcp trust port** command to disable the DHCP trusted interface of the AP for the IPv4 address.
- Before disabling STA address learning, run the **undo learn-client-address dhcp-strict** command to disable strict STA IPv4 address learning.

Precautions

- 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.

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
```

Related Topics

11.1.152 display vap-profile

11.7.45 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.

Precautions

MAC addresses and OUIs share the specifications of a STA whitelist. A maximum of 3276 MAC addresses or OUIs can be added to a STA 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
```

Related Topics

11.7.26 display sta-whitelist-profile

11.7.46 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.	-

Parameter	Description	Value
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.	-
ssid name *ssid*	Deletes an authorized SSID.	The value must be an existing SSID.
ssid *ssid*	Adds an authorized SSID.	The value must be an existing SSID.
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 countered. However, there may be APs of other vendors or 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.

For example, APs of other vendors are deployed on the existing WLAN to expand network capacity. To prevent the APs from being countered, 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.

Precautions

If you add or delete an entry, the device will re-check the validity of the unauthorized APs. If an unauthorized AP becomes authorized, the device stops countering the AP. If an authorized AP becomes unauthorized, the device starts countering the AP.

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 huawei
[HUAWEI-wlan-wids-whitelist-huawei] permit-ap mac-address 0011-2233-4455
[HUAWEI-wlan-wids-whitelist-huawei] permit-ap oui 00-11-22
[HUAWEI-wlan-wids-whitelist-huawei] permit-ap ssid huawei
```

Related Topics

11.7.82 wids-whitelist-profile (WLAN view)

11.7.47 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.	-
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

Application 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 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 must be WPA2–AES in the security profile.

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.

Only the AP2X30DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP8030DN, AP2050DN AP2050DN-E AP8130DN-W AP7030DE, AP9330DN, AP8130DN, AD9430DN-24 (including the mapping RUs), AD9430DN-12 (including the mapping RUs), AD9431DN-24X (including the mapping RUs), AP9131DN and AP9132DN AP4030TN, AP4050DN-E, AP4050DN-HD, AP6050DN, AP6150DN, AP7050DN-E, AP7050DE, AP4050DN, AP4051DN, AP4151DN, AP4050DN-S, AP8050DN, AP8150DN, AP8050DN-S, AP1050DN-S, AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, AP8182DN support the PMF function.

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 abcdffffg aes
[HUAWEI-wlan-sec-prof-p1] pmf optional
```

11.7.48 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
```

Related Topics

11.7.27 display wlan ids attack-detected

11.7.49 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
```

Related Topics

11.7.28 display wlan ids attack-detected statistics

11.7.50 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
```

Related Topics

11.7.29 display wlan ids attack-history

11.7.51 reset wlan ids device-detected

Function

The **reset wlan ids device-detected** command deletes information about the wireless devices detected.

Format

reset wlan ids device-detected { **all** | [**interference** | **rogue**] **ap** | [**rogue**] **bridge** | [**rogue**] **client** | **adhoc** | **ssid** [*ssid*] | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes information about all the wireless devices detected.	-
interference	Deletes information about the interfering devices detected.	-
rogue	Deletes information about the rogue devices detected.	-
ap	Deletes information about the APs detected.	-
bridge	Deletes information about the bridge devices detected.	-
client	Deletes information about the user terminals detected.	-

Parameter	Description	Value
adhoc	Deletes information about detected user terminals that belong to Adhoc network.	-
ssid [*ssid*]	Deletes information about detected devices with specified SSID or all SSIDs.	The value must be an existing SSID.
mac-address *mac-address*	Deletes information about detected devices with specified MAC addresses.	The value must be an existing MAC address.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When there is excessive information about wireless devices recorded or the recorded information is useless, you can run the **reset wlan ids device-detected** command to delete the information.

Precautions

The **reset wlan ids device-detected ssid** *ssid* command cannot delete device information containing special characters (such as tabs) from the SSID. To delete such information, run the **reset wlan ids device-detected mac-address** *mac-address* or **reset wlan ids device-detectedall** command.

Example

# Delete information about all the wireless devices detected.

```
<HUAWEI> reset wlan ids device-detected all
```

11.7.52 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 recollect the dynamic blacklist information, run the **reset wlan dynamic-blacklist all** command to delete all information in the dynamic blacklist. After that, the AC recollects 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 MAC address **78AC-C0C1-C1FC** from the dynamic blacklist.

```
<HUAWEI> reset wlan dynamic-blacklist mac-address 78ac-c0c1-c1fc
```

11.7.53 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.	-
client	Deletes historical records of rogue user terminals.	-
adhoc	Deletes historical records of rogue Adhoc devices.	-
ssid [*ssid*]	Deletes historical records of devices with specified SSIDs.	The value must be an existing SSID.
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
```

11.7.54 security dot1x

Function

The **security dot1x** command configures pre-shared key (PSK) authentication and encryption for WPA and WPA2.

The **undo security** command restores the default security policy.

By default, the security policy is open system.

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 passing the authentication, STAs can use the AES or TKIP algorithm for data encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

WPA/WPA2 authentication includes WPA/WPA2 PSK authentication and 802.1x authentication, which are also called WPA/WPA2 personal edition and WPA/WPA2 enterprise edition respectively. 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 are available, you can configure the WPA-WPA2 and TKIP-CCMP security policy for authentication and data encryption.

The **security wpa-wpa2 dot1x tkip aes** command indicates that WPA and WPA2 use TKIP and AES for data encryption, respectively.

Precautions

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
Warning:  If the wmm disable command, TKIP, WEP, or radio type of 802.11a/b/g is
 configured, the function of denying access of legacy STAs cannot take effect.
```

# 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
```

```
Warning:  If the wmm disable command, TKIP, WEP, or radio type of 802.11a/b/g is
 configured, the function of denying access of legacy STAs cannot take effect.
```

# Configure WPA/WPA2 (802.1x authentication and AES-TKIP encryption).

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa-wpa2 dot1x aes-tkip
Warning:  If the wmm disable command, TKIP, WEP, or radio type of 802.11a/b/g is
 configured, the function of denying access of legacy STAs cannot take effect.
```

11.7.55 security psk

Function

The **security psk** command configures pre-shared key authentication and encryption for WPA and WPA2.

The **undo security** command restores the default security policy.

By default, the security policy is open system.

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. User terminals can be authenticated using WPA or WPA2.	-
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. 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 **abc123 ABC**, enter **"abc123 ABC"**. **NOTE** To improve security, you are advised to configure a password 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 passing the authentication, user terminals can use the AES or TKIP algorithm for data encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

WPA/WPA2 authentication includes WPA/WPA2 pre-shared key authentication and 802.1X authentication, which are also called WPA/WPA2 personal edition and WPA/WPA2 enterprise edition respectively. 802.1X authentication is of high security and is applicable to enterprise networks.

To access a WLAN device using WPA or WPA2 pre-shared key authentication, run the **security psk** command. If multiple types of user terminals 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

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 pre-shared key authentication and TKIP or AES-TKIP encryption for WPA/WPA2 is configured, the access of non-HT STAs fails to be denied.

Example

# Configure WPA pre-shared key 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 abcdfffffg123 aes
```

# Configure WPA2 pre-shared key 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 abcdfffffg123 aes
```

# Configure WPA-WPA2 pre-shared key authentication and TKIP-CCMP encryption.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa-wpa2 psk pass-phrase abcdfffffg123 aes-tkip
Warning:  If the wmm disable command, TKIP, WEP, or radio type of 802.11a/b/g is
 configured, the function of denying access of legacy STAs cannot take effect.
```

11.7.56 security wapi

Function

The **security wapi** command configures the WAPI authentication mode.

The **undo security** command restores the default security policy.

By default, the security policy is open system.

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 64 characters in plain text or 48 or 68 or 88 or 108 characters in cipher text. In hex mode, the key is a string of 8 to 32 hexadecimal numbers, in which case the length of the string must be an even, or a string of 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 **abc123 ABC**, enter **"abc123 ABC"**. **NOTE** To improve security, you are advised to configure a password 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

Application 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 AP7030DE, AP7050DE and AP9330DN do not support WAPI.

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 testpassword123
```

11.7.57 security wep

Function

The **security wep** command configures the WEP authentication mode.

The **undo security** command restores the default security policy.

By default, the security policy is open system.

Format

security { **open** | **wep** [**share-key**] }

undo security

Parameters

Parameter	Description	Value
open	Sets the WEP authentication mode to open authentication.	-
wep	Sets the WEP authentication mode to share-key authentication.	-
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.	-

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. You can run this command to set the WEP authentication mode to open authentication or share-key authentication.

Table 11-193 Comparing authentication modes

Configuration	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	WEP encryption	Service data is WEP-encrypted.	STA identities are not checked, bringing security risks.
security wep share-key	Shared key authentication	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.

Precautions

- If the **security wep** [**share-key**] command is executed, you can run the **11.7.78 wep key** command to configure the pre-shared key. Otherwise, the default pre-shared key is used.
- If the **security open** command is executed, you do not need to configure the pre-shared key. The configured pre-shared key will not take effect.
- Each AP can have at most four key indexes configured. The key indexes used by different VAPs cannot be the same. That is, at most four VAPs can be configured on an AP using the **security wep** [**share-key**] command.
- The system displays the message only when the security profile has been bound to the other profiles.
- If WEP shared key authentication mode is configured, the access of non-HT STAs fails to be denied.

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
Warning:  If the wmm disable command, TKIP, WEP, or radio type of 802.11a/b/g is
 configured, the function of denying access of legacy STAs cannot take effect.
```

Related Topics

11.7.78 wep key

11.7.58 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 (" ").
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]
```

Related Topics

11.7.23 display security-profile

11.7.59 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.

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
```

Related Topics

11.7.58 security-profile (wlan view)

11.1.152 display vap-profile

11.7.60 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 office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids attack detect enable spoof
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name huawei
[HUAWEI-wlan-wids-prof-huawei] spoof-detect quiet-time 300
```

Related Topics

11.7.79 wids attack detect enable

11.7.61 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	Configure 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	Delete 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.

Example

# Configure a fuzzy matching rule using the regular expression **^HUAWE[1l]$** to identify spoofing IDs **HUAWE1** or **HUAWEl** similar to **HUAWEI**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-spoof-profile name huawei
[HUAWEI-wlan-wids-spoof-huawei] spoof-ssid fuzzy-match regex ^HUAWE[1l]$
```

Related Topics

11.7.86 wids-spoof-profile (WLAN view)

11.7.62 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 **11.7.64 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.

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
```

Related Topics

11.7.64 sta-mac

11.7.63 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 multiple 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 **11.7.62 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]
```

Related Topics

11.7.62 sta-access-mode

11.7.24 display sta-blacklist-profile

11.7.64 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 MAC address or all 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 four 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

Blacklist profile view, 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.

MAC addresses and OUIs share the specifications of a STA whitelist. A maximum of 3276 MAC addresses or OUIs can be added to a STA whitelist.

You can configure a maximum of 3276 STA MAC addresses in a STA blacklist profile.

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 MAC address 2C27-D720-746B of a STA to blacklist **huawei**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-blacklist-profile name sta-blacklist-profile1
[HUAWEI-wlan-blacklist-prof-sta-blacklist-profile1] sta-mac 2C27-D720-746B
```

Related Topics

11.7.24 display sta-blacklist-profile

11.7.26 display sta-whitelist-profile

11.7.65 sta-whitelist-profile

Function

The **sta-whitelist-profile** command creates a STA whitelist profile for VAPs or displays the STA whitelist profile view.

The **undo sta-whitelist-profile** command deletes a specified STA whitelist profile or all STA whitelist profiles for VAPs.

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 (" ").
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 **11.7.62 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]
```

Related Topics

11.7.62 sta-access-mode

11.7.26 display sta-whitelist-profile

11.7.66 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
```

11.7.67 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
```

11.7.68 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
```

11.7.69 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 the AC certificate issuer.	-
format pkcs12	Imports a certificate in P12 format.	-
format pem	Imports a certificate in PEM format.	-

Parameter	Description	Value
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.
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, run the **wapi import certificate** command to specify the AC certificate, certificate of the AC certificate issuer, 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 TFTP. 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 certificate with the same name but different contents has 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
```

11.7.70 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 of the device, and import the private key file using TFTP.
- 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
```

Related Topics

11.7.23 display security-profile

11.7.71 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 **11.7.72 wapi msk** and **11.7.75 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
```

Related Topics

11.7.72 wapi msk

11.7.75 wapi usk

11.7.72 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 MCK, 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 **11.7.71 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
```

Related Topics

11.7.71 wapi key-update

11.7.73 wapi sa-timeout

Function

The **wapi sa-timeout** command sets the timeout period of a security association (SA) of key encryption.

The **undo wapi sa-timeout** command restores the default timeout period of a SA for key encryption.

By default, the timeout period for a SA is 60s.

Format

wapi sa-timeout *sa-time*

undo wapi sa-timeout

Parameters

Parameter	Description	Value
sa-time	Specifies the timeout period of an SA.	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 timeout period of an SA to 100s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi sa-timeout 100
```

11.7.74 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
```

11.7.75 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 **11.7.71 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
```

Related Topics

11.7.71 wapi key-update

11.7.76 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 office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids attack detect enable weak-iv
[HUAWEI-wlan-group-radio-office/0] quit
[HUAWEI-wlan-ap-group-office] quit
[HUAWEI-wlan-view] wids-profile name huawei
[HUAWEI-wlan-wids-prof-huawei] weak-iv-detect quiet-time 300
```

Related Topics

11.7.79 wids attack detect enable

11.7.77 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. That is, at most four VAPs can be configured on an AP using the **security wep** [**share-key**] command.
- 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
```

Related Topics

11.7.78 wep key

11.7.78 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*

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 **abc123**

Parameter	Description	Value
		ABC, enter **"abc123 ABC"**.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

To connect to a WLAN device in WEP shared-key authentication 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
```

Related Topics

11.7.77 wep default-key

11.7.79 wids attack detect enable

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 **undo wids attack detect enable** command disables attack detection on all l 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 **undo wids attack detect enable** 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 AP radios.

Format

wids attack detect enable { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** }

undo wids attack detect enable { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** }

Parameters

Parameter	Description	Value
all	Enables all attack detection functions.	-
flood	Enables flood attack detection.	-
weak-iv	Enables weak IV attack detection.	-
spoof	Enables spoofing attack detection.	-
wpa-psk	Enables brute force attack detection for WPA-PSK authentication.	-
wpa2-psk	Enables brute force attack detection for WPA2-PSK authentication.	-
wapi-psk	Enables brute force attack detection for WAPI-PSK authentication.	-
wep-share-key	Enables brute force attack detection for 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**, **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.

Follow-up Procedure

Run the **11.7.38 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

# Enable brute force attack detection for WPA-PSK authentication on radio 0 in AP group **office**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids attack detect enable wpa-psk
```

Related Topics

11.7.38 dynamic-blacklist enable

11.7.80 wids contain enable

Function

(AP group radio view) The **wids contain enable** command enables rogue device containment on all specified radios in an AP group.

(AP group radio view) The **undo wids contain enable** command disables rogue device containment on all specified radios in an AP group.

(AP radio view) The **wids contain enable** command enables rogue device containment on an AP radio.

(AP radio view) The **undo wids contain enable** command cancels the configuration of the rogue 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 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 devices pose serious security threats to enterprise networks.

After the containment mode is set against rogue APs, the monitor AP uses the identity of the rogue AP to broadcast disauthentication frames to forcibly disconnect STAs. To prevent the STAs from connecting to the rogue AP again, the monitor AP will periodically and continuously send disauthentication frames.

After the containment mode is set against rogue STAs or ad-hoc devices, the monitor AP uses the MAC address of a rogue device to continuously send unicast disauthentication frames.

Precautions

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

After command **keep-service enable** is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue 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 device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue 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 **11.7.9 contain-mode** command to set the rogue device containment mode.

Example

# Enable rogue device containment on radio 0 in AP group **office**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids contain enable
```

Related Topics

11.7.9 contain-mode

11.7.81 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

Application 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 command **keep-service enable** is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue 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 device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue 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.

Example

# Enable device detection on radio 0 in AP group **office**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] wids device detect enable
```

11.7.82 wids-whitelist-profile (WLAN view)

Function

The **wids-whitelist-profile** command creates a WIDS whitelist profile and displays the WIDS whitelist profile view.

The **undo wids-whitelist-profile** command deletes a WIDS whitelist profile.

By default, no WIDS whitelist profile exists in the system.

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 (" ").
all	Deletes all WIDS whitelist profiles.	-

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 a WIDS whitelist profile using the **wids-whitelist-profile** command, run the **11.7.46 permit-ap** command to configure an authorized AP list.

Follow-up Procedure

Run the **11.7.83 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 **office**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-whitelist-profile name office
[HUAWEI-wlan-wids-whitelist-office]
```

Related Topics

11.7.83 wids-whitelist-profile (WIDS profile view)

11.7.46 permit-ap

11.7.83 wids-whitelist-profile (WIDS profile view)

Function

The **wids-whitelist-profile** command binds a WIDS whitelist profile to a WIDS profile.

The **undo wids-whitelist-profile** command unbinds a WIDS whitelist profile from a WIDS profile.

By default, no WIDS whitelist profile is bound to a WIDS profile.

Format

wids-whitelist-profile *profile-name*

undo wids-whitelist-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a WIDS whitelist profile.	The WIDS whitelist profile must already exist.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

After you create a WIDS whitelist profile using the **11.7.82 wids-whitelist-profile (WLAN view)** command, bind it to a WIDS profile so that the WIDS whitelist profile can take effect.

Example

# Bind the WIDS whitelist profile **office01** to the WIDS profile **wids-office01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-whitelist-profile name office01
[HUAWEI-wlan-wids-whitelist-office01] quit
```

```
[HUAWEI-wlan-view] wids-profile name wids-office01
[HUAWEI-wlan-wids-prof-wids-office01] wids-whitelist-profile office01
```

Related Topics

11.7.82 wids-whitelist-profile (WLAN view)

11.7.84 wids-profile (WLAN view)

11.7.84 wids-profile (WLAN view)

Function

The **wids-profile** command creates a WIDS profile and displays 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 **11.7.18 display wids-profile** command to view 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 (" ").
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 a WIDS profile using the **wids-profile** command, you can configure APs to detect and counter rogue devices, and detect attacks in the profile.

Follow-up Procedure

Run the **11.7.85 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]
```

Related Topics

11.7.85 wids-profile (AP group view and AP view)

11.7.85 wids-profile (AP group view and AP view)

Function

The **wids-profile** command binds a WIDS profile to an AP group or AP.

The **undo wids-profile** command unbinds a WIDS profile from an AP group or AP.

By default, no WIDS profile is bound to an AP, but the WIDS profile **default** is bound to the AP group.

Format

wids-profile *profile-name*

undo wids-profile

Parameters

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

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

After you create a WIDS profile using the **11.7.84 wids-profile (WLAN view)** command, bind it to an AP group or AP to make the profile take effect.

Example

# Bind the WIDS profile **office01** to AP group **AP-office01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-profile name office01
[HUAWEI-wlan-wids-prof-office01] quit
[HUAWEI-wlan-view] ap-group name AP-office01
[HUAWEI-wlan-ap-group-AP-office01] wids-profile office01
```

# Bind the WIDS profile **office01** to the AP with ID **1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-profile name office01
[HUAWEI-wlan-wids-prof-office01] quit
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] wids-profile office01
```

Related Topics

11.7.84 wids-profile (WLAN view)

11.7.86 wids-spoof-profile (WLAN view)

Function

The **wids-spoof-profile** command creates a WIDS spoof SSID profile and displays the WIDS spoof SSID profile view.

The **undo wids-spoof-profile** command deletes a WIDS spoof SSID profile.

By default, no WIDS spoof SSID profile exists in the system.

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 (" ").
all	Deletes all WIDS spoof SSID profiles.	-

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 a WIDS spoof SSID profile using the **wids-spoof-profile** command, run the **11.7.61 spoof-ssid** command to configure a fuzzy matching rule to identify spoofing SSIDs.

Follow-up Procedure

Run the **11.7.87 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]
```

Related Topics

11.7.87 wids-spoof-profile (WIDS profile view)

11.7.61 spoof-ssid

11.7.87 wids-spoof-profile (WIDS profile view)

Function

The **wids-spoof-profile** command binds a WIDS spoof SSID profile to a WIDS profile.

The **undo wids-spoof-profile** command unbinds a WIDS spoof SSID profile from a WIDS profile.

By default, no WIDS spoof SSID profile is bound to a WIDS profile.

Format

wids-spoof-profile *profile-name*

undo wids-spoof-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a WIDS spoof SSID profile.	The WIDS spoof SSID profile must already exist.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

After you create a WIDS spoof SSID profile using the **11.7.86 wids-spoof-profile (WLAN view)** command, bind it to a WIDS profile so that the WIDS spoof SSID profile can take effect.

Example

# Bind the WIDS spoof SSID profile **office01** to the WIDS profile **office01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-spoof-profile name office01
[HUAWEI-wlan-wids-spoof-office01] quit
[HUAWEI-wlan-view] wids-profile name office01
[HUAWEI-wlan-wids-prof-office01] wids-spoof-profile office01
```

Related Topics

11.7.86 wids-spoof-profile (WLAN view)

11.7.84 wids-profile (WLAN view)

11.7.88 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** [**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.	-
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 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 interrupted services. Users cannot associate with the AP when its radio is working in monitoring 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 -.

Only the AP2010DN, AP4030TN, AP8130DN, and AP8130DN-W support the inter-band scanning mode. Radio 1 does not support inter-band scanning.

Example

# Set the working mode of radio 0 in AP group **office** to **monitor**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name office
[HUAWEI-wlan-ap-group-office] radio 0
[HUAWEI-wlan-group-radio-office/0] work-mode monitor
Warning: Modify the work mode may cause business interruption, continue?[y/n]
:y
```

11.7.89 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 **11.7.90 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 huawei
[HUAWEI-wlan-sec-prof-huawei] wpa ptk-update enable
```

Related Topics

11.7.90 wpa ptk-update ptk-update-interval

11.7.90 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 30 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 **11.7.89 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 huawei
[HUAWEI-wlan-sec-prof-huawei] wpa ptk-update ptk-update-interval 50000
```

Related Topics

11.7.89 wpa ptk-update enable

11.8 WLAN WDS Configuration Commands

11.8.1 Command Support

Only the S5720HI supports WLAN-AC commands.

11.8.2 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
```

Related Topics

11.8.21 wds-profile

11.8.3 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 11-194 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.

Parameter	Description
Reference name	Name of the profile to which the WDS profile is bound. ● Run the **11.8.22 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 **11.8.23 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.

Related Topics

11.8.5 display wds-profile

11.8.22 wds-profile radio

11.8.23 wds-profile (AP group radio view or AP radio view)

11.8.4 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 11-195 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 **11.8.25 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.

Related Topics

11.8.6 display wds-whitelist-profile

11.8.24 wds-whitelist-profile

11.8.25 wds-whitelist-profile (AP group radio view or AP radio view)

11.8.5 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 11-196 Description of the **display wds-profile all** command output

Item	Description
Profile name	WDS profile name. To create a WDS profile, run the **11.8.21 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
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 11-197 Description of the **display wds-profile name** command output

Item	Description
WDS name	WDS name. To set a WDS name, run the **11.8.20 wds-name** command.
WDS work mode	WDS working mode. To set the WDS working mode, run the **11.8.19 wds-mode** command.
Security profile	Security profile bound to a WDS profile. To bind a security profile to a WDS profile, run the **11.8.13 security-profile (WDS profile view)** command.
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 **11.8.2 dhcp trust port (WDS profile view)** command.
MU-MIMO	Whether the MU-MIMO function is enabled. To configure the parameter, run the **11.1.199 mu-mimo disable** command.
Tagged vlan	VLAN configured in a WDS profile. To configure a VLAN in a WDS profile, run the **11.8.17 vlan tagged (WDS profile view)** command.

Item	Description
Priority map trust	Priority mapping trusted by the WDS air interface. To configure the parameter, run the **11.8.12 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 **11.8.11 priority-map dscp (WDS profile view)** command.
Beacon 2.4G rate	Transmit rate of 2.4 GHz Beacon frames configured in the WDS profile. To configure the parameter, run the **11.1.54 beacon-2g-rate** command.
Beacon 5G rate	Transmit rate of 5 GHz Beacon frames configured in the WDS profile. To configure the parameter, run the **11.1.55 beacon-5g-rate** command.

Related Topics

11.8.2 dhcp trust port (WDS profile view)

11.8.13 security-profile (WDS profile view)

11.8.17 vlan tagged (WDS profile view)

11.8.19 wds-mode

11.8.20 wds-name

11.8.6 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 11-198 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 **11.8.24 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         1047-80b1-56a0
------------------------------------------------------------------------------
Total: 1
```

Table 11-199 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 **11.8.10 peer-ap mac (WDS whitelist profile view)** command.

Related Topics

11.8.24 wds-whitelist-profile

11.8.10 peer-ap mac (WDS whitelist profile view)

11.8.7 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.

Parameter	Description	Value
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               60DE-4474-964D  0
1     AP2           0  13        wds               60DE-4474-964C  0
0     AP1           0  14        wds               60DE-4476-E36D  1
0     AP1           0  13        wds               60DE-4476-E36C  1
--------------------------------------------------------------------------------
Total: 4
```

Table 11-200 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.

Item	Description
WDS name	WDS name. To set a WDS name, run the **11.8.20 wds-name** command.
BSSID	MAC address of a VAP.
WDS links	Number of WDS links.

Related Topics

11.8.8 display wlan wds link

11.8.20 wds-name

11.8.8 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 11-201 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.
TSNR	Total SNR of a WDS link.
SNR(Ch0~3:dB)	SNR of each spatial stream of a WDS link.

Related Topics

11.8.7 display wds vap

11.8.9 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,

- On a common AP: Its GE interfaces work in **root** mode, Ethernet interfaces in **endpoint** mode, and Eth-Trunk interfaces in **root** mode.
- On a central AP: Its uplink GE interfaces in **root** mode and downlink GE interfaces work in **middle** mode.
- On an R230D: Its Ethernet interface works in **root** mode.
- On an R240D: Its Ethernet interface works in **endpoint** mode and GE interface in **root** mode.
- On an R250D, R250D-E, AP2050DN, and AP2050DN-E: Their uplink GE interfaces work in **root** mode and downlink GE interfaces in **endpoint** mode.
- On an R450D: Its GE interface works in **root** mode.

NOTE

You cannot change the working mode of wired interfaces on the R230D, R240D, R250D, R250D-E, R450D, AP2050DN, AP2050DN-E, AP2010DN and AP2030DN.

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 computer.	-
middle	Sets the working mode of an AP wired interface to middle, which can 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

The AP's wired interface supports user isolation in endpoint or middle mode, but not in root 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. When the AP's wired interface works in endpoint mode, the PVID can be configured directly. When 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
```

Related Topics

11.1.291 wired-port-profile (WLAN view)

11.8.10 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 **0001-0001-0001** 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 0001-0001-0001
[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
```

Related Topics

11.8.24 wds-whitelist-profile

11.8.11 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 11-202 describes the mapping from DSCP priorities to 802.11e user priorities by default.

Table 11-202 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
```

Related Topics

11.8.12 priority-map trust (WDS profile view)

11.8.12 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
```

Related Topics

11.8.11 priority-map dscp (WDS profile view)

11.8.13 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 huawei@123 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
```

Related Topics

11.7.58 security-profile (wlan view)

11.8.21 wds-profile

11.8.14 stp enable (AP wired port profile view)

Function

The **stp enable** command enables STP on an AP's wired interface.

The **undo stp enable** command disables STP on an AP's wired interface.

By default, STP is disabled on an AP's wired interface.

Format

stp enable

undo stp enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this 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. An STP-enabled AP does not forward STP packets to the wireless side. STP takes effect only on the AP's wired side.

Precautions

If an AP's wired interface is added to an Eth-Trunk, the wired interface does 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
```

Related Topics

11.1.291 wired-port-profile (WLAN view)

11.8.15 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.

The AP's wired interface has been configured to work in endpoint 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
```

Related Topics

11.1.291 wired-port-profile (WLAN view)

11.8.16 vlan pvid (AP wired port profile view)

Function

The **vlan pvid** command sets the PVID for an AP wired interface.

The **undo vlan pvid** command deletes the PVID of an AP wired interface.

By default, no PVID is configured for an AP wired interface.

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

The APs on the WLAN WDS network only process tagged packets.

When receiving an untagged packet from a peer device, the AP 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.

NOTE

In the following paragraphs, packets sent by the AP's wired interface refer to the management packets and service packets sent in the tunnel forwarding mode.

- After the **management-vlan** *vlan-id* command is executed, to configure the AP wired interface to allow packets carrying the management VLAN tag to pass through, run the **vlan tagged** *vlan-id* command to add the AP wired interface to the management VLAN in tagged mode.
- After the **management-vlan** *vlan-id* command is executed, to disable packets sent from the AP wired interface from carrying the management VLAN tag, run the **vlan untagged** *vlan-id* command to add the AP wired interface to the management VLAN in untagged mode.
- After the **management-vlan** *vlan-id* command is executed, to add the management VLAN tag to untagged packets received on the AP wired interface, run the **vlan pvid** *vlan-id* command to set the PVID of the AP wired interface to the management VLAN ID.

Precautions

Eth-Trunk member interfaces do not support PVID setting.

The PVID can be configured in different modes for an AP's wired interface.

- If 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.

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
```

Related Topics

11.1.291 wired-port-profile (WLAN view)

11.8.17 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 equal to or greater than 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
```

Related Topics

11.8.21 wds-profile

11.8.18 vlan (AP wired port profile view)

Function

The **vlan** command configures the VLAN to which an AP wired interface belongs.

The **undo vlan** command deletes the VLAN to which an AP wired interface belongs.

By default, an AP wired interface allows packets from all VLANs to pass. The wired interface is added to VLAN 1 in untagged mode and to other VLANs in tagged mode.

NOTE

An AP 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 the VLANs to which the AP 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.

NOTE

After an AP wired interface is added to the management VLAN, CAPWAP packets sent from the AP wired interface carry the VLAN tag.

- After the **management-vlan** *vlan-id* command is executed, to configure the AP wired interface to allow packets carrying the management VLAN tag to pass through, run the **vlan tagged** *vlan-id* command to add the AP wired interface to the management VLAN in tagged mode.
- After the **management-vlan** *vlan-id* command is executed, to disable packets sent from the AP wired interface from carrying the management VLAN tag, run the **vlan untagged** *vlan-id* command to add the AP wired interface to the management VLAN in untagged mode.
- After the **management-vlan** *vlan-id* command is executed, to add the management VLAN tag to untagged packets received on the AP wired interface, run the **vlan pvid** *vlan-id* command to set the PVID of the AP wired interface to the management VLAN ID.

Configuration Impact

If the VLAN of an AP wired interface configured using the **vlan untagged** *vlan-id* command is the same as the management VLAN configured using the **management-vlan** *vlan-id* command, you must restart the AP to make the configuration take effect.

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
```

Related Topics

11.1.291 wired-port-profile (WLAN view)

11.8.19 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
```

Related Topics

11.8.21 wds-profile

11.8.20 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 **11.8.20 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
```

Related Topics

11.8.21 wds-profile

11.8.21 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 **11.8.20 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
```

Related Topics

11.8.20 wds-name

11.8.22 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
```

Related Topics

11.8.21 wds-profile

11.8.23 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 **11.8.22 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
```

Related Topics

11.8.21 wds-profile

11.8.22 wds-profile radio

11.8.24 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 **11.8.10 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 **0001-0001-0001** 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 0001-0001-0001
[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
```

Related Topics

11.8.10 peer-ap mac (WDS whitelist profile view)

11.8.21 wds-profile

11.8.25 wds-whitelist-profile (AP group radio view or AP radio view)

11.8.25 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 **0001-0001-0001** 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 0001-0001-0001
[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
```

Related Topics

11.8.21 wds-profile

11.8.24 wds-whitelist-profile

11.9 WLAN Mesh Configuration Commands

11.9.1 Command Support

Only the S5720HI supports WLAN-AC commands.

11.9.2 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
```

Related Topics

11.9.18 mesh-profile

11.9.3 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 11-203 Description of the **display mesh-profile all** command output

Item	Description
Profile name	Mesh profile name. To create a Mesh profile, run the **11.9.18 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
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
------------------------------------------------------------------------------
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 11-204 Description of the **display mesh-profile name** command output

Item	Description
Mesh handover profile	Mesh handover profile bound to a Mesh profile. To bind a Mesh handover profile to a Mesh profile, run the **11.10.10 mesh-handover-profile (Mesh profile view)** command.
Security profile	Security profile bound to a Mesh profile. To bind a security profile to a Mesh profile, run the **11.9.28 security-profile (Mesh profile view)** command.
Mesh ID	Mesh ID of a Mesh profile. To set a Mesh ID, run the **11.9.17 mesh-id** command.
Max link number	Maximum number of Mesh links allowed on an AP. To set the maximum number of Mesh links, run the **11.9.16 max-link-number** command.
Link RSSI threshold	RSSI threshold of a Mesh link. To set the RSSI threshold of a Mesh link, run the **11.9.15 link-rssi-threshold** command.
Link report interval	Interval for reporting Mesh link information. To set the interval for reporting Mesh link information, run the **11.9.14 link-report-interval** command.
Link aging timeout	Aging time of a Mesh link. To set the aging time of a Mesh link, run the **11.9.13 link-aging-time** command.
FWA switch	FWA status in a Mesh profile. ● enable: The FWA is enabled. ● disable: The FWA is disabled. To configure FWA, run the **11.9.12 fwa enable** command.

Item	Description
FWA EDCA mode	EDCA mode. - auto: indicates the automatic mode. - manual: indicates the manual mode. To set the EDCA mode, run the **11.9.11 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 enable a DHCP trusted port in a Mesh profile, run the **11.9.2 dhcp trust port (Mesh profile view)** command.
Priority map trust	Priority mapping trusted by the Mesh air interface. To configure the parameter, run the **11.9.27 priority-map trust (Mesh profile view)** command.
Priority map mode	Mapping from DSCP priorities to 802.11e user priorities on the Mesh air interface. To configure the parameter, run the **11.9.26 priority-map dscp (Mesh profile view)** command.
Client mode	Whether to enable the Mesh client mode. - enable: The Mesh client mod is enabled. - disable: The Mesh client mod is disabled.
Beacon-2g-rate	Transmit rate of 2.4 GHz Beacon frames configured in the WDS profile. To configure the parameter, run the **11.1.54 beacon-2g-rate** command.
Beacon-5g-rate	Transmit rate of 5 GHz Beacon frames configured in the WDS profile. To configure the parameter, run the **11.1.55 beacon-5g-rate** 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 (ECWmax). ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **11.9.10 fwa wmm edca-client** command.
ECWmin	Exponent form of the minimum contention window (ECWmin). ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **11.9.10 fwa wmm edca-client** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure the parameter, run the **11.9.10 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 the parameter, run the **11.9.10 fwa wmm edca-client** command.

Related Topics

11.9.2 dhcp trust port (Mesh profile view)

11.9.10 fwa wmm edca-client

11.9.11 fwa wmm edca-mode

11.9.12 fwa enable

11.9.14 link-report-interval

11.9.15 link-rssi-threshold

11.9.16 max-link-number

11.9.17 mesh-id

11.9.28 security-profile (Mesh profile view)

11.9.4 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 11-205 Description of the **display mesh-whitelist-profile all** command output

Item	Description
Profile name	Name of a Mesh whitelist profile. To create a Mesh whitelist profile, run the **11.9.22 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        dcd2-fcf4-64a0
1        e468-a34f-6b00
----------------------------------------------------------------------------
Total: 2
```

Table 11-206 Description of the **display mesh-whitelist-profile name** command output

Item	Description
Index	Mesh whitelist ID in a Mesh whitelist profile.
MAC	MAC address on a Mesh whitelist. To add a MAC address to a Mesh whitelist, run the **11.9.25 peer-ap mac (Mesh whitelist profile view)** command.

Related Topics

11.9.22 mesh-whitelist-profile

11.9.25 peer-ap mac (Mesh whitelist profile view)

11.9.5 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 the **display mesh vap** 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           60DE-4474-964F WPA2-PSK   0
0     AP1           0    16   mesh           60DE-4474-964F Open       0
--------------------------------------------------------------------------------
Total: 2
```

Table 11-207 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 set a Mesh ID, run the **11.9.17 mesh-id** command.
BSSID	MAC address of a VAP.
Auth type	Authentication type.
Mesh links	Number of Mesh links.

Related Topics

11.9.8 display wlan mesh link

11.9.17 mesh-id

11.9.6 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 11-208 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 **11.9.19 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 **11.9.20 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.
WLAN ID	WLAN ID to which a Mesh profile is bound.

Related Topics

11.9.3 display mesh-profile

11.9.19 mesh-profile radio

11.9.20 mesh-profile (AP group radio view or AP radio view)

11.9.7 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 11-209 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 bind a Mesh whitelist profile to a Mesh profile, run the **11.9.23 mesh-whitelist-profile (AP group radio view or AP radio view)** command in the Mesh profile view.

Related Topics

11.9.4 display mesh-whitelist-profile

11.9.22 mesh-whitelist-profile

11.9.23 mesh-whitelist-profile (AP group radio view or AP radio view)

11.9.8 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* }

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.

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(Ch0~3:dB)
--------------------------------------------------------------------------------------------------------------------
----
a858-40dd-ef80  area_2          dcd2-fc04-b500  0  3    6     node    normal         -40   -20   1    17   59
56/55/-/-
area_2          a858-40dd-ef80  a858-40dd-ef80  0  3    6     portal  normal         -48   -7    0    18   45
34/35/44/-
--------------------------------------------------------------------------------------------------------------------
----
Total: 2
```

Table 11-210 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.
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(Ch0~3:dB)	SNR of each spatial stream of a Mesh link.

Related Topics

11.9.5 display mesh vap

11.9.9 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
------------------------------------------------------------------------------
ap1/60de-4474-9640/MP/0               ap2/60de-4476-e360/MPP/0
------------------------------------------------------------------------------
Total: 1
```

Table 11-211 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.

11.9.10 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 11-212 lists the default EDCA parameter settings.

Table 11-212 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

Packet Type	Parameters	Description
	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.	-
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.

Parameter	Description	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 11-213 describes the EDCA parameters.

Table 11-213 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.

Parameter	Meaning
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 11-214** shows the configuration of EDCA parameters in voice scenarios, and **Table 11-215** shows the configuration in voice and video hybrid scenarios.

Table 11-214 Recommended configuration of EDCA parameters in voice 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	5
	TXOPLimit	0
AC_BK	ECWmax	10
	ECWmin	8

Packet Type	Parameters	Description
	AIFSN	12
	TXOPLimit	0

Table 11-215 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
	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
```

Related Topics

11.9.11 fwa wmm edca-mode

11.9.11 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 auto. In automatic EDCA mode, ATs automatically adjust EDCA parameters based on the number of ATs connecting to the remote AP.	-
manual	Sets the EDCA mode to manual. In manual mode, you can run the **11.9.10 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, ATs automatically adjust EDCA parameters based on the number of ATs connecting to the remote AP. In manual mode, you can run the **11.9.10 fwa wmm edca-client** command to configure EDCA parameters of the AT. The remote AP 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 **11.9.12 fwa enable** command.
- In automatic EDCA mode, the EDCA parameters manually configured using the **11.9.10 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 huawei
[HUAWEI-wlan-mesh-prof-huawei] fwa wmm edca-mode auto
```

Related Topics

11.9.12 fwa enable

11.5.31 wmm edca-ap

11.9.12 fwa enable

Function

The **fwa enable** command enables FWA for a Mesh profile.

The **undo fwa enable** command disables FWA for a Mesh profile.

By default, FWA is disabled for a Mesh profile.

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 the connected users. You need to configure Mesh service on the remote AP and enable Fixed Wireless Access (FWA) in the Mesh profile so that the AT can connect to the remote AP.

Configuration Impact

- FWA and vehicle-ground fast link handover are mutually exclusive in a Mesh profile.
- After you enable FWA for a Mesh profile using the **fwa enable** command, the default value of *link-num* in the **max-link-number** *link-num* command is 32, and the value ranges from 1 to 32.
- After you enable FWA in a Mesh profile using the **fwa enable** command, the RSSI threshold of a Mesh link is fixed as -90 dBm, and not changed by the **11.9.15 link-rssi-threshold** command.
- After you enable FWA in a Mesh profile using the **fwa enable** command, you can complete Mesh service configuration without the need to bind a Mesh whitelist profile to the Mesh profile.
- After you enable FWA for a Mesh profile using the **fwa enable** command, the radio bound to the Mesh profile allows access from only ATs. Do not enable FWA when ATs are not used to prevent 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
```

11.9.13 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 60 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. The default value is 60.

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
```

Related Topics

11.9.18 mesh-profile

11.9.14 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
```

Related Topics

11.9.18 mesh-profile

11.9.15 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
```

Related Topics

11.9.18 mesh-profile

11.9.16 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
```

Related Topics

11.9.18 mesh-profile

11.9.17 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 **11.9.17 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
```

Related Topics

11.9.18 mesh-profile

11.9.18 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 **11.9.17 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
```

Related Topics

11.9.17 mesh-id

11.9.19 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.

On a triple-radio AP, radio 2 does not support the Mesh function.

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
```

Related Topics

11.9.18 mesh-profile

11.9.20 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.

On a triple-radio AP, radio 2 does not support the Mesh function.

This command has the same function as the **11.9.19 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
```

Related Topics

11.9.18 mesh-profile

11.9.19 mesh-profile radio

11.9.21 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** in the AP system profile.

Format

mesh-role { **mesh-portal** | **mesh-node** }

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.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

APs on a Mesh network can be sorted into the following types:

- MP (mesh-node): Any Mesh points (MPs) that can support AP functions. They provide both Mesh service and user access service.
- 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 according to service requirements. If an AP needs to provide Mesh and user access services, set the Mesh role of the AP to **mesh-node**. If an AP is located at Mesh network ingress or needs to connect MPs 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 user access services 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
```

11.9.22 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 **11.9.25 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
```

Related Topics

11.9.25 peer-ap mac (Mesh whitelist profile view)

11.9.18 mesh-profile

11.9.23 mesh-whitelist-profile (AP group radio view or AP radio view)

11.9.23 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.

On a triple-radio AP, radio 2 does not support the Mesh function.

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
```

Related Topics

11.9.18 mesh-profile

11.9.22 mesh-whitelist-profile

11.9.24 mpp-active-reselection enable

Function

The **mpp-active-reselection enable** command enables active MPP reselection.

The **undo mpp-active-reselection** command disables active MPP reselection.

By default, active MPP reselection is disabled.

Format

mpp-active-reselection enable

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, and the numbers of link hops and Mesh links. If a more preferable MPP is available, the MP selects the MPP as its Mesh gateway.

By default, active MPP reselection is disabled, and an MP can only passively reselect MPPs. Only 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 MP triggers the MPP reselection process.

Precautions

The configuration does not take effect on MPPs or vehicle-mounted APs in train-ground communication scenarios because the vehicle-mounted APs select MPPs based on the fast link handover algorithm.

Active MPP reselection will cause service loss. Configure the function according to actual needs.

Example

# Enable 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 enable
```

Related Topics

11.9.18 mesh-profile

11.9.15 link-rssi-threshold

11.9.25 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

The maximum number of MAC addresses in the Mesh whitelist is 64.

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
```

Related Topics

11.9.22 mesh-whitelist-profile

11.9.26 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 11-216 describes the mapping from DSCP priorities to 802.11e user priorities by default.

Table 11-216 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.

Parameter	Description	Value
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 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
```

Related Topics

11.9.27 priority-map trust (Mesh profile view)

11.9.27 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
```

Related Topics

11.9.26 priority-map dscp (Mesh profile view)

11.9.28 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 huawei@123 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
```

Related Topics

11.9.18 mesh-profile

11.7.58 security-profile (wlan view)

11.9.29 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.

Only the AP8130DN-W support the 4.9 GHz frequency band.

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 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 out of the channel range reselected using DFS.

The following table lists channels and frequency distribution of the 4.9 GHz frequency band.

Channel No.	Parameters	Description
184	Frequency Band	4.9G
	Center Frequency (MHz)	4920
	Upper Frequency (MHz)	4910
	Lower Frequency (MHz)	4930
188	Frequency Band	4.9G
	Center Frequency (MHz)	4940
	Upper Frequency (MHz)	4930
	Lower Frequency (MHz)	4950
192	Frequency Band	4.9G
	Center Frequency (MHz)	4960
	Upper Frequency (MHz)	4950
	Lower Frequency (MHz)	4970
196	Frequency Band	4.9G
	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 huawei
[HUAWEI-wlan-regulate-domain-huawei] wideband enable
Warning: To use the 4.9 GHz frequency band, you must apply for a license from th
e related dept. When the 4.9 GHz frequency band takes effect, the AP will be res
et. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment.done.
```

Related Topics

11.1.77 country-code

11.2.25 dca-channel bandwidth

11.10 Vehicle-Ground Fast Link Handover Configuration Commands

11.10.1 Command Support

Only the S5720HI supports WLAN-AC commands.

11.10.2 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

Only the AP9132DN and AP8182DN support this function.

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
```

Related Topics

11.1.120 display ap-system-profile

11.10.3 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

You cannot configure the Mesh client mode and bind the Mesh profile to a Mesh handover profile at the same time.

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
```

Related Topics

11.2.3 air-scan-profile

11.10.4 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 11-217 Description of the **display mesh-handover-profile all** command output

Item	Description
Profile name	Name of a Mesh handover profile. To create a Mesh handover profile, run the **11.10.9 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
------------------------------------------------------------------------------
```

Table 11-218 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 the parameter, run the **11.10.7 location-based-algorithm enable** command.
Handover probe interval	Mesh link probe interval. To configure the parameter, run the **11.10.8 link-probe-interval** command.

Related Topics

11.10.7 location-based-algorithm enable

11.10.9 mesh-handover-profile

11.10.5 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 value is an integer that ranges from 0 to 2. ● 0: indicates the 2.4 GHz radio. ● 1: indicates the 5 GHz radio. ● 2: indicates the 5 GHz radio. **NOTE** Radio 0 of the AP8130DN, AP6052DN, AP7052DN, AP7152DN, AP7052TN, AP8182DN and AP8130DN-W supports the 2.4 GHz and 5 GHz frequency bands but can only work on one frequency band at a time. Radio 0 and Radio 1 of the AP4030TN supports the 2.4 GHz and 5 GHz frequency bands but can only work on one frequency band at a time. You can run the **11.1.169 frequency** command to change the working frequency band of radio 0.

Parameter	Description	Value
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 of 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_1/60de-4476-e360/0/1      -/dcd2-fc21-5d40/-           -43   20:55:16
------------------------------------------------------------------------------
Total: 1
```

Table 11-219 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 (-).

Item	Description
Neighbor AP/MAC/Location-ID	AP 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.

11.10.6 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 11-220 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 bind a Mesh handover profile to a Mesh profile, run the **11.10.10 mesh-handover-profile (Mesh profile view)** command in the Mesh profile view.

Related Topics

11.10.4 display mesh-handover-profile

11.10.9 mesh-handover-profile

11.10.10 mesh-handover-profile (Mesh profile view)

11.10.7 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 underline (_), 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
```

Related Topics

11.10.9 mesh-handover-profile

11.10.8 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 6,000, 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 handovers, 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.

Example

# Set the Mesh link probe interval to 150 ms in Mesh handover profile **huawei**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name huawei
[HUAWEI-wlan-mesh-handover-huawei] link-probe-interval 150
```

Related Topics

11.10.9 mesh-handover-profile

11.10.9 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
```

Related Topics

11.10.10 mesh-handover-profile (Mesh profile view)

11.10.10 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
```

Related Topics

11.10.9 mesh-handover-profile

11.11 IoT AP Configuration Commands

11.11.1 Command Support

- Only the S5720HI supports WLAN-AC commands.
- IoT AP configuration commands take effect only for the AP4050DN-E, AP7052DN, AP7152DN, and R250D-E.

11.11.2 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** }

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.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an IoT card communicates with an AP through the serial interface, the communication rate between the IoT card and AP does not exceed the maximum baud rate of the serial interface, that is, 115200 bit/s. This connection type is applicable to scenarios without high traffic volume. When an IoT card communicates with an AP through an Ethernet interface, the communication rate of 10 Mbit/s is supported. This connection mode is applicable to electronic shelf label (ESL) scenarios.

Precautions

The modified connection type takes effect only after the AP is restarted.

Currently, only the AP4050DN-E supports this command.

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
```

11.11.3 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
```

11.11.4 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

Parameters	Description	Value
ap-id	Specifies the AP ID.	The AP ID must exist.
all	Specifies all AP cards.	-
card-number	Specifies the number of an interface on an IoT card.	The interface number must exist.

Parameters	Description	Value
usb	Specifies the USB interface on an IoT card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to query 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} command and restart the device.
--------------------------------------------------------------------------------
 Card                    : 1
--------------------------------------------------------------------------------
 IOT card status         : absent
--------------------------------------------------------------------------------
 Card                    : 2
--------------------------------------------------------------------------------
 IOT card status         : present
 Card connect type       : Serial
 Connected status        : mismatch
 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
--------------------------------------------------------------------------------
 Card                    : 3
--------------------------------------------------------------------------------
 IOT card status         : absent
--------------------------------------------------------------------------------
 Card                    : usb
--------------------------------------------------------------------------------
 USB status              : disabled
 IOT card status         : absent
--------------------------------------------------------------------------------
```

Table 11-221 Description of the **display ap card** command output

Item	Description
IOT card status	Card status. ● Present: An IoT card is installed. ● absent: No IoT card is installed.
Card connect 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.
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, and 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.
USB status	Actual working status of the USB function on an AP.

11.11.5 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.

No result is displayed for a card if it 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 displa
yed. To modify the effective connection type, run the card connect-type {serial|ethernet} command and
restart the device.
--------------------------------------------------------------------------------------------------------------------------------
------
------------
AP ID  Card-number    Wireless-standard    Vendor-name    Card-type      Card-connect-type  Connected-
status  Serial-number

--------------------------------------------------------------------------------------------------------------------------------
------
------------
2      1              RFID                 ENJOYOR        TOEAPV1.2      ethernet(up)       match
0000000000000001
--------------------------------------------------------------------------------------------------------------------------------
------
------------
Total: 1
```

Table 11-222 Description of the **display ap-card all** command output

Item	Description
AP ID	AP ID.
Card-number	Card ID.
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 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.
Serial-number	Module ID of the card. The value is a 16-byte BCD character set.

11.11.6 display iot-profile

Function

The **display iot-profile** command displays the configuration of a specified IoT profile or all IoT profiles.

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 configuration of a specified IoT profile or all IoT profiles.

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 11-223 Description of the **display iot-profile all** command output

Item	Description
Profile name	IoT profile name

Item	Description
Reference	Number of times an IoT profile is referenced.

# Display configuration information about 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
Share key                     : ******
------------------------------------------------------------------------------
```

Table 11-224 Description of the **display iot-profile name wlan-IoT** command output

Item	Description
Type	Card type. To configure this parameter, run the **11.11.24 type (IoT profile view)** command.
Agent permit IP address	IP address of a trusted host computer. To configure this parameter, run the **11.11.3 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 **11.11.3 config-agent permit ip-address** command.
Management server IP address	IP address of the host computer. To configure this parameter, run the **11.11.17 management-server** command.
Management server port	Port number of the host computer. To configure this parameter, run the **11.11.17 management-server** command.
Share key	Shared key. To configure this parameter, run the **11.11.21 share-key** command.

Related Topics

11.11.3 config-agent permit ip-address

11.11.17 management-server

11.11.21 share-key

11.11.7 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 IoT profile **wlan-IoT**.

```
<HUAWEI> display references iot-profile name wlan-IoT
-------------------------------------------------------------------------------
Reference type    Reference name                     Reference card
-------------------------------------------------------------------------------
AP group          ap-group1                          Card-1
-------------------------------------------------------------------------------
Total:1
```

Table 11-225 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.

11.11.8 display references serial-profile

Function

The **display references serial-profile** command displays reference information about an IoT card serial profile.

Format

display references serial-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a serial profile.	The serial 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 card serial profile.

Example

# Display reference information about serial profile **wlan-serial**.

```
<HUAWEI> display references serial-profile name wlan-serial
--------------------------------------------------------------------------------
```

```
Reference type     Reference name                    Reference card
-------------------------------------------------------------------------------
AP group           ap-group1                         Card-1
-------------------------------------------------------------------------------
Total:1
```

Table 11-226 Description of the **display references serial-profile name wlan-serial** command output

Item	Description
Reference type	Type of the profile to which the serial profile is bound.
Reference name	Name of the profile to which the serial profile is bound.
Reference card	Card to which the serial profile is bound.

11.11.9 display serial-profile

Function

The **display serial-profile** command displays configuration information about a specified IoT card serial profile or all serial profiles.

Format

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

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a serial 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 serial profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view the configuration information about a specified IoT card serial profile or all serial profiles.

Example

# Display the configuration of all serial profiles.

```
<HUAWEI> display serial-profile all
--------------------------------------------------------------------------------
Profile name                      Reference
--------------------------------------------------------------------------------
profile1                        1
wlan-serial                      1
preset-enjoyor-toeap              13
--------------------------------------------------------------------------------
Total:3
```

Table 11-227 Description of the **display serial-profile all** command output

Item	Description
Profile name	Profile name.
Reference	Number of times a serial profile is referenced.

# Display configuration information about serial profile **wlan-serial**.

```
<HUAWEI> display serial-profile name wlan-serial
--------------------------------------------------------------------------------
Speed(Unit:bps)             : 19200
Parity                      : odd
Stop bits                   : 2
Frame format                : frame-start-stop
Frame length(Unit:Byte)     : 270
Frame start                 : 0xbb
Frame stop                  : 0xcc
--------------------------------------------------------------------------------
```

Table 11-228 Description of the **display serial-profile name wlan-serial** command output

Item	Description
Speed(Unit:bps)	Baud rate in bps. To configure this parameter, run the **11.11.22 speed (serial profile view)** command.
Parity	Parity bit. To configure this parameter, run the **11.11.18 parity (serial profile view)** command.
Stop bits	Stop bits. To configure this parameter, run the **11.11.23 stopbits (serial profile view)** command.
Frame format	Frame format. To configure this parameter, run the **11.11.10 frame-format (serial profile view)** command.
Frame length(Unit:Byte)	Frame length in byte. To configure this parameter, run the **11.11.11 frame-length (serial profile view)** command.
Frame start	Frame start flag. To configure this parameter, run the **11.11.12 frame-start (serial profile view)** command.
Frame stop	Frame stop flag. To configure this parameter, run the **11.11.13 frame-stop (serial profile view)** command.

Related Topics

11.11.22 speed (serial profile view)

11.11.18 parity (serial profile view)

11.11.23 stopbits (serial profile view)

11.11.10 frame-format (serial profile view)

11.11.11 frame-length (serial profile view)

11.11.12 frame-start (serial profile view)

11.11.13 frame-stop (serial profile view)

11.11.10 frame-format (serial profile view)

Function

The **frame-format** command configures the format for serial frames on an IoT card interface.

The **undo frame-format** command restores the configured format for serial frames to the default value.

By default, the frame format is **frame-start-stop**.

Format

frame-format { **fixed-length** | **frame-start-stop** }

undo frame-format

Parameters

Parameter	Description	Value
fixed-length	Specifies a fixed frame length.	-
frame-start-stop	Specifies the start and stop flags for frames.	-

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If parameter settings in preset profiles cannot meet your needs, you can create new serial profiles, customize serial communication parameters and framing parameters, and apply the settings to IoT card interfaces.

Precautions

If the serial frame length on an IoT card interface is set to 1 byte using the **11.11.11 frame-length (serial profile view)** command, the serial frame format must be **fixed-length**.

Example

# Configure a fixed-length frame format.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] serial-profile name profile1
[HUAWEI-wlan-serial-prof-profile1] frame-format fixed-length
```

Related Topics

11.11.11 frame-length (serial profile view)

11.11.12 frame-start (serial profile view)

11.11.13 frame-stop (serial profile view)

11.11.11 frame-length (serial profile view)

Function

The **frame-length** command configures the length for serial frames on an IoT card interface.

The **undo frame-length** command restores the configured length for serial frames to the default value.

By default, the frame length is 512 bytes.

Format

frame-length *frame-length-value*

undo frame-length

Parameters

Parameter	Description	Value
frame-length-value	● If the frame format adopts a fixed length, this parameter is used for framing. ● If the frame format is set to frame-start-stop, this parameter specifies the maximum frame length used to verify the validity of framing.	The value is an integer that ranges from 1 to 280, in bytes.

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If parameter settings in preset profiles cannot meet your needs, you can create new serial profiles, customize serial communication parameters and framing parameters, and apply the settings to IoT card interfaces.

Precautions

If the serial frame format on an IoT card interface is set to **frame-start-stop** using the **11.11.10 frame-format (serial profile view)** command, the serial frame length must be at least 2 bytes.

Example

# Set the frame length to 270 bytes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] serial-profile name profile1
[HUAWEI-wlan-serial-prof-profile1] frame-length 270
```

Related Topics

11.11.10 frame-format (serial profile view)

11.11.12 frame-start (serial profile view)

11.11.13 frame-stop (serial profile view)

11.11.12 frame-start (serial profile view)

Function

The **frame-start** command configures the start flag byte for serial frames on an IoT card slot.

The **undo frame-start** command restores the configured start flag byte to the default value.

By default, the start flag byte is aa.

Format

frame-start *frame-start-value*

undo frame-start

Parameters

Parameter	Description	Value
frame-start-value	Specifies the start flag byte of a frame.	The value ranges from 0 to ff.

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If parameter settings in preset profiles cannot meet your needs, you can create new serial profiles, customize serial communication parameters and framing parameters, and apply the settings to IoT card slots.

Prerequisites

This parameter is valid only when the frame format is set to **frame-start-stop**.

Example

# Set the start flag byte to **bb**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] serial-profile name profile1
[HUAWEI-wlan-serial-prof-profile1] frame-start bb
```

Related Topics

11.11.10 frame-format (serial profile view)

11.11.11 frame-length (serial profile view)

11.11.13 frame-stop (serial profile view)

11.11.13 frame-stop (serial profile view)

Function

The **frame-stop** command configures the stop flag byte for serial frames on an IoT card slot.

The **undo frame-stop** command restores the configured stop flag byte to the default value.

By default, the stop flag byte is 7e.

Format

frame-stop *frame-stop-value*

undo frame-stop

Parameters

Parameter	Description	Value
frame-stop-value	Specifies the stop flag byte of a frame.	The value ranges from 0 to ff.

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If parameter settings in preset profiles cannot meet your needs, you can create new serial profiles, customize serial communication parameters and framing parameters, and apply the settings to IoT card slots.

Prerequisites

This parameter is valid only when the frame format is set to **frame-start-stop**.

Example

# Set the stop flag byte to **ff**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] serial-profile name profile1
[HUAWEI-wlan-serial-prof-profile1] frame-stop ff
```

Related Topics

11.11.10 frame-format (serial profile view)

11.11.11 frame-length (serial profile view)

11.11.12 frame-start (serial profile view)

11.11.14 card

Function

The **card** command displays the IoT card interface view.

Format

card { *card-number* | **usb** }

Parameters

Parameter	Description	Value
card-number	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

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

Only the AP4050DN-E, AP7052DN, AP7152DN, and R250D-E support IoT cards connected to USB interfaces.

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 group1
[HUAWEI-wlan-ap-group-group1] card 1
[HUAWEI-wlan-group-card-group1/1]
```

11.11.15 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]
```

11.11.16 iot-profile (IoT card interface view)

Function

The **iot-profile** command binds an IoT profile.

The **undo iot-profile** command deletes an IoT profile.

By default, no IoT profile is bound to an IoT card interface.

Format

iot-profile *profile-name* **config-agent** { **udp-port** *udp-port* | **tcp-port** *tcp-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 (" ").
config-agent udp-port *udp-port*	Specifies the UDP port number.	The value is an integer that ranges from 1025 to 55535. **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.
config-agent tcp-port *tcp-port*	Specifies the TCP port number. When the card type is **cas-edu**, this parameter is not supported.	The value is an integer that ranges from 1025 to 55535. **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

The IoT card interface corresponds to the local UDP and TCP port numbers when the IoT profile is bound and the AP functions as a server.

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 group1
[HUAWEI-wlan-ap-group-group1] card 1
[HUAWEI-wlan-group-card-group1/1] iot-profile profile1 config-agent udp-port 50200
```

11.11.17 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 server-ip *server-ip* **server-port** *server-port-num*

undo management-server server-ip *server-ip* [**server-port** *server-port-num*]

Parameters

Parameter	Description	Value
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 1025 to 55535.

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 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 RFID 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 multiple host computers are configured, the device automatically select one available host computer for link establishment rather than establish links with multiple host computers.

Example

# Configure the IP address and port number of 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
```

11.11.18 parity (serial profile view)

Function

The **parity** command configures the parity bit for serial data on an IoT card slot.

The **undo parity** command restores the configured parity bit to the default value.

By default, the parity bit is set to **none** on an IoT card slot.

Format

parity { **none** | **odd** | **even** | **mark** | **space** }

undo parity

Parameters

Parameter	Description	Value
none	Indicates no parity.	-
odd	Indicates odd parity.	-
even	Indicates even parity.	-
mark	Indicates mark parity.	-
space	Indicates space parity.	-

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If parameter settings in preset profiles cannot meet your needs, you can create new serial profiles, customize serial communication parameters and framing parameters, and apply the settings to IoT card slots.

Example

# Set parity to odd parity.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] serial-profile name profile1
[HUAWEI-wlan-serial-prof-profile1]parity odd
```

11.11.19 serial-profile (WLAN view)

Function

The **serial-profile** command creates a serial profile and displays the serial profile view.

The **undo serial-profile** command deletes a serial profile.

By default, serial profile **preset-enjoyor-toeap** is bound to an IoT card interface.

Format

serial-profile name *profile-name*

undo serial-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a serial 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 serial profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If parameter settings in preset profiles cannot meet your needs, you can create new serial profiles, customize serial communication parameters and framing parameters, and apply the settings to IoT card slots. User-defined profiles cannot start with "preset-".

Precautions

Preset serial profiles can be bound to facilitate the card configuration. A preset profile name is in the format of "preset-vendor name-model", which cannot be modified or deleted. User-defined profiles cannot start with "preset-".

Example

# Create serial profile **profile1** and display the serial profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] serial-profile name profile1
[HUAWEI-wlan-serial-prof-profile1]
```

11.11.20 serial-profile (IoT card interface view)

Function

The **serial-profile** command binds a serial profile to an AP or AP group.

The **undo serial-profile** command deletes the serial profile bound to an AP or AP group.

By default, serial profile **preset-enjoyor-toeap** is bound to an AP group, and no serial profile is bound to an AP.

Format

serial-profile *profile-name*

undo serial-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a serial 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 (" ").

Views

IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If parameter settings in preset profiles cannot meet your needs, you can create new serial profiles, customize serial communication parameters and framing parameters, and apply the settings to IoT card slots.

Example

# Bind serial profile **profile1** to AP group **group1**.

```
<HUAWEI>system-view
[HUAWEI]wlan
[HUAWEI-wlan-view]ap-group name group1
[HUAWEI-wlan-ap-group-group1]card 1
[HUAWEI-wlan-group-card-group1/1]serial-profile profile1
```

11.11.21 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
```

11.11.22 speed (serial profile view)

Function

The **speed** command configures the baud rate for serial communications on an IoT card slot.

The **undo speed** command restores the configured baud rate to the default value.

By default, the baud rate is 115,200 bit/s.

Format

speed *speed-value*

undo speed

Parameters

Parameter	Description	Value
speed-value	Specifies the baud rate for serial communication on an IoT card slot.	The unit is bit/s and the value can be: • 9600 bit/s • 19200 bit/s • 38400 bit/s • 57600 bit/s • 115200 bit/s

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IoT card and an AP communicate with each other in serial mode. Each IoT card interface uses independent serial communication parameters and framing parameters. By default, an IoT card interface is bound with the preset serial profile **preset-enjoyor-toeap**.

Example

# Set the baud rate to **57600 bit/s**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] serial-profile name profile1
[HUAWEI-wlan-serial-prof-profile1] speed 57600
```

11.11.23 stopbits (serial profile view)

Function

The **stopbits** command configures stop bits for serial data on an IoT card slot.

The **undo stopbits** command restores the configured stop bits to the default value.

The default stop bit is 1.

Format

stopbits { **1** | **2** }

undo stopbits

Parameters

Parameter	Description	Value
1	Specifies one stop bit.	-
2	Specifies two stop bits.	-

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If parameter settings in preset profiles cannot meet your needs, you can create new serial profiles, customize serial communication parameters and framing parameters, and apply the settings to IoT card slots.

Example

# Set two stop bits.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] serial-profile name profile1
[HUAWEI-wlan-serial-prof-profile1] stopbits 2
```

11.11.24 type (IoT profile view)

Function

The **type** command sets the type for 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	Specifies an IoT card that complies with IoT standards of the China Academy of Science.	-
common	Specifies an IoT card that complies with Huawei's IoT standards.	-

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When Huawei ACs are used in 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 **11.11.16 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 **11.11.3 config-agent permit ip-address** and **11.11.21 share-key** commands cannot be executed.

Example

# Set the type of an IoT card 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, other configuration items in the profile are cleared.Continue?[Y/
N]:y
```

Related Topics

11.11.6 display iot-profile

11.11.25 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 **11.11.2 card connect-type ethernet** command.

Example

# Bind AP wired port profile **wired-port1** to IoT card 1.

```
<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] card 1
[HUAWEI-wlan-group-card-group1/1] wired-port-profile wired-port1
```

Related Topics

11.11.2 card connect-type

11.12 WLAN Traffic Optimization Commands

11.12.1 Command Support

Only the S5720HI supports WLAN-AC commands.

11.12.2 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-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
ap-name *ap-name*	Specifies an AP name.	The AP name 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 11-229 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	Percentage of current multicast users against the maximum number of multicast users that is configured globally.

11.12.3 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 AC collects statistics on the current multicast bandwidth of the VAP according to the bandwidth of global multicast groups configured for the AP, 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
```

Related Topics

11.12.4 igmp-snooping max-bandwidth (traffic profile view)

11.12.4 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 kbps.

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 **11.12.3 igmp-snooping group-bandwidth (AP system profile view)** command to configure the bandwidth of global multicast groups on the AP.

Example

# Set the maximum multicast bandwidth to 500 kbps 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
```

Related Topics

11.12.3 igmp-snooping group-bandwidth (AP system profile view)

11.12.5 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

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.

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
```

11.12.6 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 on the device 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 **11.5.23 traffic-profile (WLAN view)** command.

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
```

11.12.7 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 message 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
```

Related Topics

8.9.3 display igmp-snooping

11.12.6 igmp-snooping enable (traffic profile view)

8.9.28 igmp-snooping querier enable

8.9.44 igmp-snooping suppress-time

11.12.8 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 on 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

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.

Example

# Set the maximum traffic volume of broadcast packets that can pass through 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
```

11.12.9 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

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.

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
```

11.12.10 traffic-optimize multicast-unicast enable

Function

The **traffic-optimize multicast-unicast enable** command enables the function of converting multicast packets to unicast packets in a traffic profile.

The **undo traffic-optimize multicast-unicast enable** command disables the function of converting multicast packets to unicast packets in a traffic profile.

By default, the function of converting multicast packets to unicast packets is disabled in a traffic profile.

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 function of converting multicast packets to unicast packets in scenarios that have high requirements on multicast stream transmission, such as a high-definition video on-demand scenario.

After the function is enabled, an AP listens on Report and Leave packets to maintain multicast-to-unicast entries. When sending multicast packets to the client, the AP converts the multicast packets to unicast packets based on the multicast-to-unicast entries to improve multicast stream transmission efficiency.

Example

# Enable the function of converting multicast packets to unicast 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 multicast-unicast enable
```

11.12.11 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.

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
```

11.12.12 traffic-optimize sta-bridge-forward disable

Function

The **traffic-optimize sta-bridge-forward disable** command forbids an air interface to forward packets to bridging terminals.

The **undo traffic-optimize sta-bridge-forward disable** command cancels of the configuration of forbidding an air interface to forward packets to bridging terminals.

By default, an air interface is allowed to forward packets to bridging terminals.

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 forbid air interfaces to forward packets to bridging terminals. This can reduce the number of packets transmitted on the air interfaces and improve the air interface performance.

Example

# Forbid an air interface to forward packets to bridging terminals 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
```

11.12.13 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

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.

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
```

11.13 WLAN Reliability Commands

11.13.1 Command Support

Only the S5720HI supports WLAN-AC commands.

11.13.2 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 the **ac protect alarm-restrain enable** 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 **11.1.277 undo ap** or **11.1.48 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
```

Related Topics

11.13.12 display ac protect

11.13.3 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
```

Related Topics

11.13.12 display ac protect

11.13.4 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 **ac protect link-switch mode** **network-stabilization** command has been run to set the active/standby link switchover mode to the network stabilization mode.

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
```

Related Topics

11.13.5 ac protect link-switch mode

11.13.6 ac protect link-switch packet-loss

11.1.120 display ap-system-profile

11.13.5 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 **11.13.9 ac protect protect-ac** and **11.13.14 priority** commands, or the **11.13.13 primary-access** and **11.13.11 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
```

Related Topics

11.13.6 ac protect link-switch packet-loss

11.13.4 ac protect link-switch packet-loss echo-probe-time

11.1.120 display ap-system-profile

11.13.6 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 **ac protect link-switch mode** **network-stabilization** command has been run to set the active/standby link switchover mode to the network stabilization mode.

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
```

Related Topics

11.13.5 ac protect link-switch mode

11.13.4 ac protect link-switch packet-loss echo-probe-time

11.1.120 display ap-system-profile

11.13.7 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
```

Related Topics

11.13.12 display ac protect

11.13.8 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
```

Related Topics

11.13.12 display ac protect

11.13.14 priority

11.13.9 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
```

Related Topics

11.13.12 display ac protect

11.13.15 protect-ac

11.13.10 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
```

Related Topics

11.13.12 display ac protect

11.13.11 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
```

Related Topics

11.13.14 priority

11.13.13 primary-access

11.13.15 protect-ac

11.13.12 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 11-230 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 **11.13.7 ac protect enable** command.
Protect AC	Standby AC IP address. To configure the parameter, run the **11.13.9 ac protect protect-ac** command.
Priority	Priority of the local AC. To configure the parameter, run the **11.13.8 ac protect priority** command.
Protect restore	Whether global revertive switching is enabled on the AC. To configure the parameter, run the **11.13.10 ac protect restore disable** command.

Item	Description
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 **11.13.3 ac protect cold-backup kickoff-station** command.
Alarm restrain	Whether to enable AP fault alarm suppression. To configure the parameter, run the **11.13.2 ac protect alarm-restrain enable** command.

Related Topics

11.13.3 ac protect cold-backup kickoff-station

11.13.7 ac protect enable

11.13.8 ac protect priority

11.13.9 ac protect protect-ac

11.13.10 ac protect restore disable

11.13.13 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
```

Related Topics

11.13.11 backup-access

11.13.14 priority

11.13.15 protect-ac

11.13.14 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
```

Related Topics

11.13.8 ac protect priority

11.1.120 display ap-system-profile

11.13.15 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 connect an AP to two ACs (active and standby ACs) to implement dual-link backup, you can run the **protect-ac** command to configure the standby AC's 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 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
```

Related Topics

11.13.9 ac protect protect-ac

11.1.120 display ap-system-profile