14 WLAN-AC Commands

About This Chapter

14.1 WLAN Service Configuration Commands
14.2 WLAN Radio Resource Management Configuration Commands
14.3 WLAN Roaming Commands
14.4 WLAN Security Configuration Commands
14.5 WLAN WDS Configuration Commands
14.6 WLAN Reliability Commands

14.1 WLAN Service Configuration Commands

14.1.1 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ac sysnetid ABC123
```

Related Topics

14.1.69 display ac global configuration

14.1.2 access-user syslog-restrain enable

Function

The **access-user syslog-restrain enable** command enables system log suppression.

 Copyright © Huawei Technologies Co., Ltd.

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
```

14.1.3 access-user syslog-restrain period

Function

The **access-user syslog-restrain period** command sets the period of system log suppression.

The **undo access-user syslog-restrain period** command restores the default period of system log suppression.

By default, the period of system log suppression is 300s.

Format

access-user syslog-restrain period *period*

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Set the period of system log suppression to 600s.

```
<Huawei> system-view
[Huawei] access-user syslog-restrain period 600
```

14.1.4 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

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 ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] active-dull-client enable
```

Related Topics

14.1.118 display ssid-profile

14.1.5 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] alarm-restriction disable
```

Related Topics

14.1.98 display ap-system-profile

14.1.6 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] alarm-restriction period 200
```

Related Topics

14.1.98 display ap-system-profile

14.1.7 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.

 Copyright © Huawei Technologies Co., Ltd.

(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*.

 Copyright © Huawei Technologies Co., Ltd.

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

Example

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

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

14.1.8 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 **14.1.10 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 anti-attack broadcast-flood disable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the broadcast flood blacklist function.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name profile1
[Huawei-wlan-vap-prof-profile1] anti-attack broadcast-flood blacklist enable
```

Related Topics

14.1.9 anti-attack broadcast-flood disable
14.1.10 anti-attack broadcast-flood sta-rate-threshold

14.1.9 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

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 ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] vap-profile name profile1
[Huawei-wlan-vap-prof-profile1] anti-attack broadcast-flood disable
```

Related Topics

14.1.10 anti-attack broadcast-flood sta-rate-threshold

14.1.10 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.

 Copyright © Huawei Technologies Co., Ltd.

If the broadcast flood blacklist function is enabled using the **14.1.8 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 anti-attack broadcast-flood disable** command.

Example

Set the broadcast flood threshold to 100 pps.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name profile1
[Huawei-wlan-vap-prof-profile1] anti-attack broadcast-flood sta-rate-threshold 100
```

Related Topics

14.1.9 anti-attack broadcast-flood disable

14.1.8 anti-attack broadcast-flood blacklist enable

14.1.11 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap auth-mode mac-auth
```

Related Topics

14.1.77 display ap global configuration

14.1.12 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 ac
[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 ac
[Huawei-wlan-view] ap blacklist mac 0025-9e07-8270 to 0025-9e07-8276
```

Related Topics

14.1.30 ap-confirm

14.1.73 display ap blacklist

 Copyright © Huawei Technologies Co., Ltd.

14.1.13 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 NMS needs to periodically query performance statistics (including AP and radio performance statistics and information about users on an AP) from an AC that queries the information from the AP.

Data caching is a method to improve query performance, in which an AC periodically queries performance statistics and caches the data. When the NMS requires the data, the NMS queries the data from the buffer but not from the AP.

You are advised to enable an AC to buffer AP data when you use the NMS to query AP statistics. When NMS query expires, the NMS can obtain AP data from the AC.

Example

Enable an AC to buffer AP data.

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

Related Topics

14.1.14 ap data-collection interval

14.1.77 display ap global configuration

 Copyright © Huawei Technologies Co., Ltd.

14.1.14 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 ac
[Huawei-wlan-view] ap data-collection enable
[Huawei-wlan-view] ap data-collection interval 57
```

Related Topics

14.1.13 ap data-collection enable

14.1.77 display ap global configuration

 Copyright © Huawei Technologies Co., Ltd.

14.1.15 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 disabled 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 Central AP or NMS can obtain Layer 2 information about the connected RRUs, including RRUs' interfaces and connections with other devices. Additionally, the Central AP or NMS can obtain details about network topology and interface changes. To view the Layer 2 link status between RRUs, and between RRUs and switch or analyze the network topology, enable WLAN LLDP.

Precautions

WLAN LLDP can be enabled in the system view and the RRU wired port link profile view.

- An RRU can send and receive LLDP packets only after LLDP is enabled in both the WLAN view and the RRU wired port link profile view.
- After LLDP is disabled in the WLAN view, the commands for enabling and disabling LLDP on the RRU wired port link profile view do not take effect.

Example

Enable LLDP in the WLAN view.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap lldp enable
```

Related Topics

14.1.77 display ap global configuration

14.1.160 lldp enable

14.1.16 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Restore the factory settings of AP **N1-2**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap manufacturer-config ap-name N1-2
Warning: Reset AP to the manufacturing default configuration, continue?[Y/N]:y
```

14.1.17 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

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

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.1.70 display ap

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

Format

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 (?) or spaces, and cannot start or end with double quotation marks (" ") or spaces.
ftp-password	Specifies the password for logging in to the FTP server.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher	Specifies the password in cipher text.	-
ftp-password	Specifies the FTP server password.	The value is a string of characters without question marks (?) or spaces. It cannot start or end with double quotation marks (" ") or spaces. *ftp-password* contains 48 or 68 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 31 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

 Copyright © Huawei Technologies Co., Ltd.

- 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 ac
[Huawei-wlan-view] ap update ftp-server ip-address 192.168.1.100 ftp-username admin ftp-password cipher wlanadmin
```

Related Topics

14.1.21 ap update mode

14.1.22 ap update multi-load

14.1.91 display ap update configuration

14.1.19 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

 Copyright © Huawei Technologies Co., Ltd.

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 5, an error message will be displayed after the first 5 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 ac
[Huawei-wlan-view] ap update ftp-server max-connect-number 10
```

Related Topics

14.1.21 ap update mode

14.1.22 ap update multi-load

14.1.91 display ap update configuration

 Copyright © Huawei Technologies Co., Ltd.

14.1.20 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

 Copyright © Huawei Technologies Co., Ltd.

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_v200r006c10.bin**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update load ap-name N1-2 update-filename fitap6x10xn_v200r006c10.bin
```

Related Topics

14.1.24 ap update reset

14.1.92 display ap update status

14.1.21 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 **ftp-mode**.

Format

ap update mode { **ftp-mode** | **sftp-mode** }

undo ap update mode

Parameters

Parameter	Description	Value
ftp-mode	Indicates the FTP mode. The AC delivers the FTP configuration to APs using the **14.1.18 ap update ftp-server** command, and APs download the upgrade version file from the FTP server.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sftp-mode	Indicates the SFTP mode. The AC delivers the SFTP configuration to APs using the **14.1.25 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 ac
[Huawei-wlan-view] ap update mode sftp-mode
Info:Changing AP update mode causes an AP update failure, continue?[Y/N]:Y
```

Related Topics

14.1.91 display ap update configuration

14.1.22 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>]

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

- If neither **ap-name** *ap-name* nor **ap-id** *ap-id* is specified, all APs in the specified AP group are upgraded.
- If APs specified by **ap-name** *ap-name* and **ap-id** *ap-id* are in different AP groups, the APs cannot be upgraded.

Prerequisites

AP upgrade files have been configured in batches using the **ap update update-filename** command.

Follow-up Procedure

Run the **ap update multi-reset** command to reset APs in batches to make AP upgrade take effect.

Precautions

The **undo ap update multi-load** command cancels batch upgrade of APs 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 ac
[Huawei-wlan-view] ap update multi-load ap-type 19
```

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

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update multi-load ap-group ap-group1
```

Related Topics

14.1.27 ap update update-filename

14.1.23 ap update multi-reset

14.1.92 display ap update status

14.1.23 ap update multi-reset

Function

The **ap update multi-reset** command resets APs of the same type 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>]

 Copyright © Huawei Technologies Co., Ltd.

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 of the same type 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

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

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

14.1.24 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Restart AP **N1-2** after the upgrade.

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.1.20 ap update load

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

Format

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.
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 (?) or spaces, and cannot start or end with double quotation marks (") or spaces.
sftp-password	Specifies the password for logging in to the sftp server.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher	Specifies the password in cipher text.	-
sftp-password	Specifies the sftp server password.	The value is a string of characters without question marks (?) or spaces. It cannot start or end with double quotation marks (" ") or spaces. *sftp-password* can be up to 68 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 31 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

 Copyright © Huawei Technologies Co., Ltd.

- 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 ac
[Huawei-wlan-view] ap update sftp-server ip-address 192.168.1.100 sftp-username admin sftp-password cipher wlanadmin
```

Related Topics

14.1.21 ap update mode

14.1.22 ap update multi-load

14.1.91 display ap update configuration

14.1.26 ap update sftp-server max-connect-number

Function

The **ap update sftp-server max-connect-number** 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap update sftp-server max-connect-number 10
```

Related Topics

14.1.21 ap update mode

14.1.22 ap update multi-load

14.1.91 display ap update configuration

 Copyright © Huawei Technologies Co., Ltd.

14.1.27 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the upgrade file name for APs with the type ID 19 to **fitap6x10xn_v200r006c10.bin**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update update-filename fitap6x10xn_v200r006c10.bin ap-type 19
```

Related Topics

14.1.22 ap update multi-load

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

Format

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.	-

Copyright © Huawei Technologies Co., Ltd.

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 32 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 or 68 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**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[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 that must contain at least one lowercase letter, one uppercase letter, and one
digit):
Confirm password:
```

Related Topics

14.1.77 display ap global configuration

14.1.93 display ap username

14.1.29 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 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.
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 value is a string of 1 to 31 characters.

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.11 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 AP is not in the whitelist, the AP can go online only after its identity is confirmed by the user using the **14.1.30 ap-confirm** command.
- When the AP authentication mode is set to SN authentication using the **14.1.11 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 AP is not in the whitelist, the AP can go online only after its identity is confirmed by the user using the **14.1.30 ap-confirm** command.

Prerequisites

The AP authentication mode has been set to MAC address or SN authentication using the **14.1.11 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 ac
[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 ac
[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 ac
[Huawei-wlan-view] ap whitelist sn 08PE56430071
```

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

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

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.95 display ap whitelist
14.1.11 ap auth-mode
14.1.30 ap-confirm

14.1.30 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 **14.1.89 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.

 Copyright © Huawei Technologies Co., Ltd.

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

Confirm all APs.

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

Related Topics

14.1.70 display ap

14.1.95 display ap whitelist

14.1.77 display ap global configuration

14.1.31 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 (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all AP groups.	-

Views

WLAN view

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.32 ap-group (AP view)** or **14.1.38 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 ac
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1]
```

Related Topics

14.1.32 ap-group (AP view)

14.1.38 ap-regroup

14.1.97 display ap-group

14.1.32 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*

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[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
```

14.1.33 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*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ap-id	Specifies the AP ID.	The value is an integer. The value range varies according to devices: ● AR150 series: 0 to 15 ● AR100series, AR120 series and AR160 series: 0 to 15 ● AR200 series: 0 to 15 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D and AR2204E: 0 to 31 ● AR2220, AR2220E, AR2230: 0 to 63 ● AR2204XE and AR2204XE-DC: 0 to 255 ● AR2240 and AR3200 series: – SRU40: 0 to 127 – SRU60: 0 to 127 – SRU80: 0 to 255 – SRU100E: 0 to 255 – SRU200 and SRU200E: 0 to 255 – SRU400: 0 to 511 ● AR2240C: 0 to 127 ● AR3600 series: 0 to 255
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 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

 Copyright © Huawei Technologies Co., Ltd.

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

To add an AP, enter the MAC address of the AP if the AP authentication mode is MAC address authentication. If the AP authentication mode is SN authentication, 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 ac
[Huawei-wlan-view] ap-id 11 type-id 19 ap-mac 0025-9e07-8270
```

Related Topics

14.1.70 display ap

14.1.34 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ap-id *ap-id*	Specifies the AP ID.	The value is an integer. The value range varies according to devices: ● AR150 series: 0 to 15 ● AR100series, AR120 series and AR160 series: 0 to 15 ● AR200 series: 0 to 15 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D and AR2204E: 0 to 31 ● AR2220, AR2220E, AR2230: 0 to 63 ● AR2204XE and AR2204XE-DC: 0 to 255 ● AR2240 and AR3200 series: – SRU40: 0 to 127 – SRU60: 0 to 127 – SRU80: 0 to 255 – SRU100E: 0 to 255 – SRU200 and SRU200E: 0 to 255 – SRU400: 0 to 511 ● AR2240C: 0 to 127 ● AR3600 series: 0 to 255
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

 Copyright © Huawei Technologies Co., Ltd.

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*] 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 ac
[Huawei-wlan-view] ap-mac 0025-9e07-8260
```

Related Topics

14.1.70 display ap

14.1.35 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the view of the AP named **area_1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-name area_1
[Huawei-wlan-area_1]
```

Related Topics

14.1.70 display ap

14.1.36 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 begin 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Change the AP name to **AP-N1-2**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 0
[Huawei-wlan-ap-0] ap-name AP-N1-2
```

14.1.37 ap-ping

Function

The **ap-ping** command uses a specified AP to ping a network device and displays the returned result.

Format

ap-ping { **ap-name** *ap-name* | **ap-id** *ap-id* } [**-c** *count* | **-s** *packetsize* | **-m** *time* | **-t** *timeout*] * *host*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of an AP used to ping other network devices.	The AP name must already exist.
ap-id *ap-id*	Specifies the ID of an AP used to ping other network devices.	The AP ID must already exist.
-c *count*	Specifies the number of ICMP Echo Request packets to be sent.	The value is an integer that ranges from 1 to 10. The default value is 4.
-s *packetsize*	Specifies the length of an Echo Request packet excluding the IP header and ICMP header.	The value is an integer that ranges from 20 to 8100, in bytes. The default value is 56 bytes.
-m *time*	Specifies the time to wait before sending the next ICMP Request packet.	The value is an integer that ranges from 1 to 5000, in milliseconds. The default value is 2000 ms.
-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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 ac
[Huawei-wlan-view] ap-ping ap-name N1-2 192.168.0.1
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
```

14.1.38 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*

 Copyright © Huawei Technologies Co., Ltd.

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.
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 **14.1.31 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 ac
[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

14.1.31 ap-group

14.1.70 display ap

 Copyright © Huawei Technologies Co., Ltd.

14.1.39 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.
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 begin 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.

Example

Change the AP name from **N1-2** to **N2-2**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-rename ap-name N1-2 new-name N2-2
```

Related Topics

14.1.70 display ap

14.1.40 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 ac
[Huawei-wlan-view] ap-reset ap-name N1-2
Warning: Reset AP(s), continue?[Y/N]:y
```

14.1.41 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** }

 Copyright © Huawei Technologies Co., Ltd.

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 begin 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 **14.1.42 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 ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1]
```

Related Topics

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

14.1.98 display ap-system-profile

14.1.42 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 **14.1.41 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create the AP system profile **ap-system1** and bind it to AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.1.31 ap-group

14.1.41 ap-system-profile (WLAN view)

14.1.108 display references ap-system-profile

14.1.43 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[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

14.1.118 display ssid-profile

14.1.44 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

Copyright © Huawei Technologies Co., Ltd.

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

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 has a fixed value of 1 Mbit/s, and *beacon-2g-rate* configured in the SSID profile view does not take effect on the AP.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] beacon-2g-rate 18
```

Related Topics

14.1.118 display ssid-profile

14.1.188 radio-type (2G radio profile view)

14.1.45 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] beacon-5g-rate 18
```

Related Topics

14.1.118 display ssid-profile

14.1.46 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 ms.

Format

beacon-interval *beacon-interval*

undo beacon-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
beacon-interval	Specifies the interval for sending Beacon frames.	The value is an integer that ranges from 60 ms to 1000 ms

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.

Example

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

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

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.47 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*

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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

14.1.100 display capwap configuration

14.1.48 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 enabled.

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

 Copyright © Huawei Technologies Co., Ltd.

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 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
```

Related Topics

14.1.100 display capwap configuration

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

Format

capwap dtls psk *psk-value*

undo capwap dtls psk

 Copyright © Huawei Technologies Co., Ltd.

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

Application Scenario

During the CAPWAP tunnel establishment between an AP and an AC, the AP performs a DTLS session with the AC as soon as the AP is associated with the AC. DTLS supports PSK encryption. When the pre-shared key is used for DTLS encryption, the **capwap dtls psk** command can be used to manually change the value in the DTLS session on the AC.

NOTE

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

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

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

Precautions

After the configuration is complete, the new pre-shared key will be automatically synchronized to online APs. However, the old pre-shared key takes effect on the APs. The new pre-shared key takes effect only after the APs goes offline and goes online again.

Example

Configure the pre-shared key for DTLS encryption as **z0020011@11**.

```
<Huawei> system-view
[Huawei] capwap dtls psk z0020011@11
Deliver DTLS PSK to devices using CAPWAP connections. It may take a few mi
nutes.
 ---------------------------------------------------------------------------
 CAPWAP DTLS PSK deliver result
 Deliver Number : 0
 Success Number : 0
 Failed  Number : 0
---------------------------------------------------------------------------
```

Related Topics

14.1.48 capwap dtls control-link encrypt

14.1.50 capwap dtls psk-mandatory-match enable

14.1.100 display capwap configuration

14.1.50 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 not allowed 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.

 Copyright © Huawei Technologies Co., Ltd.

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

14.1.100 display capwap configuration

14.1.51 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** }

 Copyright © Huawei Technologies Co., Ltd.

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.
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. If an AP goes offline unexpectedly, you can set a larger CAPWAP

 Copyright © Huawei Technologies Co., Ltd.

heartbeat detection interval and a larger number of CAPWAP heartbeat detections.

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

14.1.47 capwap control-link-priority

14.1.100 display capwap configuration

14.1.52 capwap ipv6 enable

Function

The **capwap ipv6 enable** command enables CAPWAP tunnels to support IPv6 functions.

The **undo capwap ipv6 enable** command disables CAPWAP tunnels from supporting IPv6 functions.

By default, CAPWAP tunnels are disabled from supporting IPv6 functions.

Format

capwap ipv6 enable

undo capwap ipv6 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, CAPWAP tunnels are disabled from supporting IPv6 functions. You can run the **capwap ipv6 enable** command to enable CAPWAP tunnels to support IPv6 functions.

Example

Enable CAPWAP tunnels to support IPv6 functions.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] capwap ipv6 enable
```

14.1.53 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 deletes the PSK for checking integrity of CAPWAP packets.

By default, no PSK is configured for checking integrity of CAPWAP packets.

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

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CAPWAP packets are transmitted between the AC and APs. This command is used to configure a PSK for checking integrity of CAPWAP packets to prevent the packets from being forged or tampered with and prevent malformed packet attacks.

NOTE

After the command is executed, all APs connected to the AC are restarted.

Example

Set the PSK for checking integrity of CAPWAP packets to **z0020011@11**.

```
<Huawei> system-view
[Huawei] capwap message-integrity psk z0020011@11
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue? [Y/N]:y
```

Related Topics

14.1.54 capwap message-integrity psk-mandatory-match enable

14.1.54 capwap message-integrity psk-mandatory-match enable

Function

The **capwap message-integrity psk-mandatory-match enable** command enables CAPWAP packets to reach the AC without integrity check.

The **undo capwap message-integrity psk-mandatory-match enable** command disables CAPWAP packets without integrity check from reaching the AC.

By default, CAPWAP packets without integrity check cannot be successfully sent to the AC.

Format

capwap message-integrity psk-mandatory-match enable

undo capwap message-integrity psk-mandatory-match enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

APs in earlier versions cannot receive the pre-shared key (PSK) for checking packet integrity from the AC. This command is used to control whether CAPWAP packets from APs in earlier versions can be successfully sent to the AC without integrity check.

NOTE

If this command is not executed, the APs that do not support packet integrity check cannot get online on the AC.

Example

Enable CAPWAP packets to reach the AC without integrity check.

```
<Huawei> system-view
[Huawei] capwap message-integrity psk-mandatory-match enable
```

Related Topics

14.1.53 capwap message-integrity psk

14.1.55 capwap sensitive-info psk

Function

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

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

By default, the default PSK is used for encrypting sensitive information.

Format

capwap sensitive-info psk *psk-value*

undo capwap sensitive-info psk

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
psk-value	Specifies the PSK for encrypting sensitive information.	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 may be exchanged between the AC and APs, for example, FTP user name/password, AP login user name/password, and service configuration PSK. By default, a PSK is used for encrypting sensitive information. This command allows users to manually modify the PSK.

NOTE

After the command is executed, all APs connected to the AC are restarted.

Precautions

In dual-link backup and HSB scenarios, the PSK for encryption must be set to the same value on the active and standby ACs. Otherwise, APs cannot set up a CAPWAP tunnel with the standby AC.

 Copyright © Huawei Technologies Co., Ltd.

Example

Modify the PSK for encrypting sensitive information to **z0020011@11**.

```
<Huawei> system-view
[Huawei] capwap sensitive-info psk z0020011@11
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue? [Y/N]:y
```

14.1.56 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.
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

 Copyright © Huawei Technologies Co., Ltd.

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

A loopback interface or VLANIF interface has been created and has an IP address configured. If the loopback or VLANIF interface uses an IPv6 address, the IPv6 address can only be configured manually.

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

14.1.100 display capwap configuration

14.1.57 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 **14.1.74 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

 Copyright © Huawei Technologies Co., Ltd.

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.	-
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*.

The 2.4 GHz radio does not support the 40 MHz Minus, 40 MHz Plus and 80 MHz bandwidth in FCC compliance regions (including America).

The channels you configure must be supported by the terminals; otherwise, the terminals cannot discover wireless signals. For example, when the country code is

 Copyright © Huawei Technologies Co., Ltd.

set to China, 5 GHz channels 36, 40, 44, 48, 52, 56, 60, and 64 can be configured. However, most terminals do not support these channels currently. If these channels are configured, the terminals cannot discover wireless signals. In this case, you can configure 5 GHz channels 149, 153, 157, 161, and 165, which are supported by the terminals.

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.

NOTE

- The 80 MHz, 160 MHz, and 80+80 MHz working bandwidths are only supported in the 5G radio view.
- Only APs that support 802.11ac support the 80 MHz parameters.

Example

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

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] channel 20mhz 6
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.58 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, the AP send an announcement when the channel is switched.

Format

channel-switch announcement disable

undo channel-switch announcement disable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

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

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

NOTE

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

Example

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

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

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.59 commit (WLAN view)

Function

The **commit** command commits configurations of a specified AP or all APs.

Format

commit { **all** | **ap-name** *ap-name* | **ap-id** { *ap-id1* [**to** *ap-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
all	Commits configurations of all APs.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ap-name *ap-name*	Commits configurations of a specified AP.	The AP name must exist.
ap-id *ap-id1*	Commits configurations of an AP with a specified ID.	The AP ID must exist.
to *ap-id2*	Specifies the end AP ID in a batch operation. The *ap-id2* value must be larger than the *ap-id1* value.	The AP ID must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can configure attributes for APs on the AC. The configurations are delivered to APs only after you run the **commit** command to commit the configurations.

NOTE

If you commit configurations to a large number of APs simultaneously, some of the APs may fail to receive the configurations. In this case, you are advised to commit the configurations again.

Example

Commit the configuration of a specified AP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] commit ap-name ap-1
Warning: Committing configuration may cause service interruption, continue?[Y/N]:y
```

Commit configurations of all APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] commit all
Warning: Committing configuration may cause service interruption, continue?[Y/N]:y
```

14.1.60 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] console disable
```

Related Topics

14.1.98 display ap-system-profile

14.1.61 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

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
country-code	Specifies a country code.	The value is a string of characters. For specific values, see **Table 14-1**.

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Table 14-1 Country codes supported by ACs

Country Code	Country/Region
AE	United Arab Emirates
AM	Armenia
AR	Argentina
AT	Austria
AU	Australia
AZ	Azerbaijan
BE	Belgium
BG	Bulgaria
BH	Bahrain
BN	Brunei Darussalam
BO	Bolivia
BR	Brazil
BY	Belarus
BZ	Belize
CA	Canada
CH	Switzerland
CL	Chile

Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
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
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

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
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	North Macedonia
MO	Macao, Special Administrative Region of China
MT	Malta
MX	Mexico
MY	Malaysia
NG	Nigeria
NL	Netherlands
NO	Norway
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PH	Philippines
PK	Pakistan
PL	Poland
PR	Puerto Rico

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
PT	Portugal
QA	Qatar
RO	Romania
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
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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[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

14.1.117 display regulatory-domain-profile

14.1.62 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] coverage distance 2
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.63 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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] cpu-usage threshold 60
```

 Copyright © Huawei Technologies Co., Ltd.

14.1.64 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*.
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, it sends an alarm message to the AC. To

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] port-link-profile name port-link1
[Huawei-wlan-port-link-prof-port-link1] crc-alarm enable
```

Related Topics

14.1.104 display port-link-profile

14.1.65 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-**

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] deny-broadcast-probe enable
```

Related Topics

14.1.118 display ssid-profile

14.1.66 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 31 case-sensitive characters without spaces.

Views

AP wired port profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] wired-port-profile name wired-port1
[Huawei-wlan-wired-port-wired-port1] description poe-power
```

Related Topics

14.1.128 display wired-port-profile

14.1.67 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 **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

 Copyright © Huawei Technologies Co., Ltd.

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, this command takes effect only on uplink interfaces of an RRU.

Example

Create the VAP profile **vap1** and configure a DHCP trusted interface on the AP in the VAP profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] dhcp trust port
```

Related Topics

14.1.127 display vap-profile

14.1.98 display ap-system-profile

14.1.68 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

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable DAI using this command to prevent Man in The Middle (MITM) attacks and theft on authorized user information. When a device receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN ID of the ARP packet with DHCP snooping binding entries. If the ARP packet matches a binding entry, the device allows the packet to pass through. If the ARP packet does not match any binding entry, the device discards the packet.

Prerequisites

Terminal address learning has been enabled on the AP's wired interface using the **learn-client-address enable** command.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

This command takes effect only on ARP packets transmitted on an AP's wired interface.

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 ac
[Huawei-wlan-view] wired-port-profile name wire1
[Huawei-wlan-wired-port-wire1] dai enable
```

Related Topics

14.1.128 display wired-port-profile

14.1.69 display ac global configuration

Function

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

Format

display ac global configuration

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display AC global configuration.

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

Table 14-2 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 **14.1.1 ac sysnetid** command.

Related Topics

14.1.1 ac sysnetid

14.1.70 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.

 Copyright © Huawei Technologies Co., Ltd.

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 in faulty state. • **idle**: Displays information about APs in idle state. • **name-conflicted**: Displays information about APs having duplicate names.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• **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.

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

 Copyright © Huawei Technologies Co., Ltd.

Display information about APs in normal state.

```
<Huawei> display ap by-state normal
AP information(State-normal):
------------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP              Type          State          STA Uptime
------------------------------------------------------------------------------------------------
0    dcd2-fcf6-76a0 area_1 ap-group1 192.168.120.254 AP6010DN-AGN  nor            0   4H:50M:55S
1    60de-4474-9640 area_2 ap-group1 192.168.120.253 AP5010DN-AGN  nor            0   6H:5M:24S
------------------------------------------------------------------------------------------------
Total: 2
```

Table 14-3 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	State of an AP. • commit-failed: WLAN service configuration commitment fails. • committing: WLAN service configuration is being committed. • config: The AP is initializing configuration. • config-failed: The AP fails to initialize the configuration. • download: The AP is downloading the upgrade software. • fault: The AP is faulty. • idle: The AP is in idle state. • name-conflicted: APs' names conflict. • nor: The AP is in normal state. • standby: The AP is on the standby AC. • ver-mismatch: Versions of the AP and AC do not match.
STA	Number of STAs connected to an AP.
Uptime	Online duration of an AP.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.33 ap-id
14.1.34 ap-mac

14.1.71 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):
--------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
SSID
------------------------------------------------------
test2
------------------------------------------------------
Total: 1
In control AP(5G):
------------------------------------------------------
SSID
------------------------------------------------------
test3
------------------------------------------------------
Total: 1
Uncontrol AP(5G):
------------------------------------------------------
SSID
------------------------------------------------------
test4
------------------------------------------------------
Total: 1
```

Table 14-4 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.

14.1.72 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

 Copyright © Huawei Technologies Co., Ltd.

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 14-5 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.

14.1.73 display ap blacklist

Function

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

 Copyright © Huawei Technologies Co., Ltd.

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 14-6 Description of the **display ap blacklist** command output

Item	Description
ID	ID of the MAC address in the AP blacklist. The ID is generated automatically when the MAC address is specified.
MAC	MAC addresses of the APs that are not allowed to connect to the AC. To add MAC addresses to the AP blacklist, run the **14.1.12 ap blacklist** command.

Related Topics

14.1.12 ap blacklist

 Copyright © Huawei Technologies Co., Ltd.

14.1.74 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 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
 WDS  mode                      : -
 Radio band                     : 2.4G
 Radio type                     : bgn
 Config channel/bandwidth       : -/20M
 Actual channel/bandwidth       : 1/20M
 Config EIRP                    : 127
```

 Copyright © Huawei Technologies Co., Ltd.

```
 Actual EIRP                 : 27
 Maximum EIRP                : 27

 VAP configurations:
  WLAN ID 1:
   SSID                     : HUAWEI-WLAN
   Authen mode              : Open
   Encrypt mode             : -
--------------------------------------------------------------------------------
Radio 1 configurations:
 Radio enable                : yes
 WDS  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
   Authen mode              : Open
   Encrypt mode             : -
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
AP system profile          : default
Regulatory domain profile  : default
WIDS profile               : default
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 Eth-trunk0      : default
Radio 0
 Radio 2.4G profile        : default
 Radio 5G profile          :
 VAP profile
  WLAN_1                   : default
```

```
 WDS profile              :
 WDS whitelist profile    :
 Radio switch             : enable
 Channel                  : -
 Channel bandwidth        : 20mhz
 EIRP(dBm)                : 127
 Antenna gain(dB)         : -
 Coverage distance(100 m) : 3
 Radio frequency          : 2.4G
 WIDS attack detect       : -
Radio 1
 Radio 2.4G profile       :
 Radio 5G profile         : default
 VAP profile
  WLAN  1                 : default
 WDS profile              :
 WDS whitelist profile    :
 Radio switch             : enable
 Channel                  : -
 Channel bandwidth        : 20mhz
 EIRP(dBm)                : 127
 Antenna gain(dB)         : -
 Coverage distance(100 m) : 3
 Radio frequency          : 5G
 WIDS attack detect       : -
------------------------------------------------------------------------------
```

Table 14-7 Description of the **display ap config-info** command output

Item	Description
AP MAC	MAC address of an AP.
AP SN	SN of an AP.
AP type	AP type.
AP name	AP name. To configure the parameter, run the **14.1.36 ap-name (AP view)** or **14.1.39 ap-rename** command.
AP group	AP group. To configure the parameter, run the **14.1.32 ap-group (AP view)** or **14.1.38 ap-regroup** command.
Country code	Country code. To configure the parameter, run the **14.1.61 country-code** command.
Radio 0 configurations/Radio 1 configurations	Radio configuration.
Radio enable	Radio status. To configure the parameter, run the **14.1.183 radio disable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
WDS mode	WDS mode. To configure the parameter, run the **14.5.18 wds-mode** command.
Radio band	Frequency band of a radio. To configure the parameter, run the **14.1.143 frequency** command.
Radio type	Protocol type of a radio.
Config channel/bandwidth	Configured AP channel and bandwidth. To configure the parameter, run the **14.1.57 channel** command.
Actual channel/bandwidth	Actual AP channel and bandwidth.
Config EIRP	Transmit power of a radio configured in the radio profile. To configure the parameter, run the **14.1.140 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 **14.1.234 vap-profile** command.
SSID	SSID name. To configure the parameter, run the **14.1.214 ssid** command.
Authen mode	Authentication mode.
Encrypt mode	Encryption mode.
AP system profile	Name of the referenced AP system profile. To configure the parameter, run the **14.1.42 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 **14.1.193 regulatory-domain-profile** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
WIDS profile	Name of the referenced WIDS profile. To configure the parameter, run the **14.4.57 wids-profile (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 **14.1.241 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 **14.1.185 radio-2g-profile** command.
Radio 5G profile	Name of the referenced 5G radio profile. To configure the parameter, run the **14.1.187 radio-5g-profile** command.
VAP profile	Name of the referenced VAP profile. To configure the parameter, run the **14.1.234 vap-profile** command.
WLAN 1	VAP profile name. To configure the parameter, run the **14.1.234 vap-profile** command.
WDS profile	Name of the referenced WDS profile. To configure the parameter, run the **14.5.21 wds-profile radio** command.
WDS whitelist profile	WDS whitelist profile referenced by an AP group. To configure the parameter, run the **14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)** command.
Radio switch	Radio status. To configure the parameter, run the **14.1.183 radio disable** command.
Channel	Working channel of a radio. To configure the parameter, run the **14.1.57 channel** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Channel bandwidth	Working bandwidth of a radio. To configure the parameter, run the **14.1.57 channel** command.
EIRP(dBm)	Transmit power of a radio, in dBm. To configure the parameter, run the **14.1.140 eirp** command.
Antenna gain(dB)	Antenna gain of a radio, in dBm. To configure the parameter, run the **14.1.7 antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter, in 100 m. To configure the parameter, run the **14.1.62 coverage distance** command.
Radio frequency	Working frequency band of a radio. To configure the parameter, run the **14.1.143 frequency** command.
WIDS attack detect	Whether attack detection is enabled. To configure the parameter, run the **14.4.55 wids attack detect enable** command.

14.1.75 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* }

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.

Copyright © Huawei Technologies Co., Ltd.

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.
2.4G 40M-: 5,6,7,8,9,10,11.
5G   20M : 36,40,44,48,52,56,60,64,149,153,157,161,165.
5G   40M+: 36,44,52,60,149,157.
5G   40M-: 40,48,56,64,153,161.
5G   80M : 36,40,44,48,52,56,60,64,149,153,157,161.
```

Table 14-8 Description of the **display ap configurable channel** command output

Item	Description
2.4G 20M	Configurable 20 MHz channels supported by the AP on the 2.4 GHz frequency band.
2.4G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 2.4 GHz frequency band.
2.4G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 2.4 GHz frequency band.
5G 20M	Configurable 20 MHz channels supported by the AP on the 5 GHz frequency band.
5G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 5 GHz frequency band.
5G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 5 GHz frequency band.
5G 80M	Configurable 80 MHz channels supported by the AP on the 5 GHz frequency band.

 Copyright © Huawei Technologies Co., Ltd.

14.1.76 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]
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 14-9 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 14-10 display ap elabel all command output

Item	Description
ID	AP ID.
MAC	MAC address of an AP.
Name	AP name.
Type	AP type.

 Copyright © Huawei Technologies Co., Ltd.

SN	SN of an AP.
Item	BOM code of an AP.

14.1.77 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

None

Example

Display AP global configuration.

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

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

Item	Description
AP auth-mode	AP authentication mode. To configure the parameter, run the **14.1.11 ap auth-mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AP LLDP swtich	Whether LLDP is enabled on an AP. To configure the parameter, run the **14.1.15 ap lldp enable** command.
AP username/password	User name and password for AP login. To configure the parameter, run the **14.1.28 ap username** command.
AP data collection	Whether data buffering is enabled on an AP. To configure the parameter, run the **14.1.13 ap data-collection enable** command.
AP data collection interval(minute)	AP data buffering duration. To configure the parameter, run the **14.1.14 ap data-collection interval** command.

Related Topics

14.1.11 ap auth-mode
14.1.15 ap lldp enable
14.1.28 ap username
14.1.13 ap data-collection enable
14.1.14 ap data-collection interval

14.1.78 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-12 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 local AP information stored on a neighboring device

Display LLDP neighbor information about GE0/0/0 of AP **huawei**.

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

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           : AR1200
                  Huawei Versatile Routing Platform Software
                  VRP (R) software,Version 5.110 (AR1200 V200R009C00)
                  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
------------------------------------------------------------------------------
```

Table 14-13 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

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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

 Copyright © Huawei Technologies Co., Ltd.

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 local device information stored on the neighbor device.
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
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

 Copyright © Huawei Technologies Co., Ltd.

Management address type	Management address type of the neighbor.
Management address	Management address of the neighbor.

Related Topics

14.1.15 ap lldp enable

14.1.79 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.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

APs' neighbor information reflects the APs' locations and neighbor relationships, helping you plan the network.

Information about authorized neighbors includes forward channel attenuation and backward channel attenuation:

 Copyright © Huawei Technologies Co., Ltd.

- Forward channel attenuation: indicates the attenuation from the local AP to the neighboring AP.
- Backward channel attenuation: indicates the attenuation from the neighboring AP to the local AP.

If a neighboring AP is an unauthorized one, the system displays only the power of signals received from the neighboring AP.

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 Front(db)  Back(db)
------------------------------------------------------------
0      1       ap-14      1       44         45
1      2       ap-14      2       44         45
------------------------------------------------------------
Total: 2

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 14-14 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.
Front(db)	Forward channel attenuation, in dB. The value is the attenuation from the local AP to the neighboring AP.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Back(db)	Backward channel attenuation, in dB. The value is the attenuation from the neighboring AP to the local AP.
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.
SSID	Service set identifier (SSID) of an unauthorized neighbor.

14.1.80 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.

 Copyright © Huawei Technologies Co., Ltd.

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    Reboot by ap-reset command
60de-4476-e360  2015-01-31/14:02:35    Reboot by ap update reset command
1047-80b1-56a0  2015-01-31/13:52:35    Reboot by ap update reset command
--------------------------------------------------------------------------------
Total records: 3
```

Table 14-15 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.

Related Topics

14.1.195 reset ap offline-record

14.1.81 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

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

If an AP fails to go online on the AC, you can run the 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 overwrites 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  In blacklist
--------------------------------------------------------------------------------
Total records: 1
```

Table 14-16 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reason	Reason for the AP online failure. • Lack of license. • Not in SN whitelist. • Not in MAC whitelist. • return "In blacklist". • MAC and SN mismatched. • Negotiation DTLS failed. • Negotiation CAPWAP tunnel failed. • Data batching. • AP IP address mismatch. • AP auto update fail. • Create link failed. • Config timeout. • Config failed. • Version mismatch. • Unsupported AP type, AC version may need to be upgraded. • Name conflict. • AP reaches the upper limit. • Capwap psk mismatch. • CAPWAP message-integrity PSK mismatch. • Forcibly disconnected in certain situations. • AP type mismatch. • DTLS negotiation failed, because of negotiation timeout or inconsistent PSKs on two ends. • Other reasons.

Related Topics

14.1.196 reset ap online-fail-record

14.1.82 display ap optical-info

Function

The **display ap optical-info** command displays optical module information.

 Copyright © Huawei Technologies Co., Ltd.

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, only the AP6610DN-AGN, AP6610DN-AGN-US, AP8030DN and AP8130DN support optical modules.

Example

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

```
<Huawei> display ap optical-info ap-name huawei
------------------------------------------------------------------------------
Common information:
  Transceiver Type                :1000_BASE_LX
  Connector Type                  :LC
  Wavelength(nm)                  :1310
  Transfer Distance(m)            :10000(9um)
  Copper Link Length(m)           :0
  Digital Diagnostic Monitoring   :NO
```

 Copyright © Huawei Technologies Co., Ltd.

```
  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
--------------------------------------------------------------------------------
```

Table 14-17 Description of the **display ap optical-info** command output

Item	Description
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Manufacturing Date	Manufacturing date of the optical module.
Temperature(degree C)	Current temperature of the optical module, in °C.
Temp High Threshold(degree C)	The upper threshold for the temperature of the optical module, in °C.
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.

 Copyright © Huawei Technologies Co., Ltd.

14.1.83 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
  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 up rate(Kbps)            : 0
  port down rate(Kbps)          : 0
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 up rate(Kbps)            : 0
  port down rate(Kbps)          : 0
--------------------------------------------------------------------------------
```

Table 14-18 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 size (KB).
Temperature(degree C)	AP's internal temperature (°C). **NOTE** The temperature cannot be viewed on the AP2010DN, AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP3010DN-AGN, AP3010DN-V2, AP5010SN-GN and AP5010DN-AGN. The value is displayed as "-".
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 that are received by the wireless interface.
Wireless port drop frames(TX)	Number of discarded data frames that are sent by the wireless interface.
Wireless port total bytes(RX)	Number of bytes received by the wireless interface.
Wireless port total bytes(TX)	Number of bytes sent by the wireless interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 that are received by the wired interface.
port drop frames(TX)	Number of discarded data frames that are sent by the wired interface.
port total Bytes(RX)	Number of bytes received by the wired interface.
port total Bytes(TX)	Number of bytes sent by the wired-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 up rate(Kbps)	Upstream rate on the wired interface, in kbit/s.
port down rate(Kbps)	Downstream rate on the wired interface, in kbit/s.

14.1.84 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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
--------------------------------------------------------------------------------------------------------------------------
-----
Total: 1
```

Table 14-19 Description of the **display ap performance statistics** command output

Parameter	Description
AP-ID	AP ID.
Port	AP port.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
State	Status of the AP port. • down: The AP port is Down. • up: The AP port is Up. • *down: indicates that 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.

14.1.85 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.

 Copyright © Huawei Technologies Co., Ltd.

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           : V200R007C00
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)     : -
IoT card status            : slot 1: -, slot 2: -, slot 3: -
------------------------------------------------------------------------------
```

Table 14-20 Description of the **display ap run-info** command output

Item	Description
AP type	AP type.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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	IP address of an AP.
IP mask	Mask of an AP.
Gateway	Gateway IP address of an AP.
DNS server	IP address of the DNS server.
GigabitEthernet port *number*	ID of the AP's Ethernet interface.
Port speed(Mbps)	Rate on the upstream Ethernet interface, in Mbit/s.
Port speed mode	Rate mode of the upstream Ethernet interface, including automatic and non-automatic negotiation modes.
Port duplex	Duplex type of the upstream Ethernet interface, including full duplex and half duplex.
Port duplex mode	Duplex mode of the upstream Ethernet interface, including automatic and non-automatic negotiation modes.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
STP down recovery time(ddd:hh:mm:ss)	Remaining recovery time of the STP.
IoT card status	IoT card status. • -: indicates that the IoT card is not in position. • present: indicates that the IoT card is in position.

14.1.86 display ap service-config acl

Function

The **display ap service-config acl** command displays the ACL configuration on a specified AP.

Format

display ap service-config acl { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

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

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can determine which ACLs have been delivered to the AP based on the command output, which helps locate and troubleshoot faults about user rights.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display ACL configuration on AP **huawei**.

```
<Huawei> display ap service-config acl ap-name huawei
-------------------------------------------------------------------------------
Index          ACL number
-------------------------------------------------------------------------------
1              3000
2              3002
3              3015
4              3022
5              3030
-------------------------------------------------------------------------------
Total: 5
```

Table 14-21 Description of the **display ap service-config acl** command output

Item	Description
Index	Index.
ACL number	ACL number configured on an AP.

14.1.87 display ap sta-signal strength

Function

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

Format

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

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the average signal strength of STAs connected to the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the average signal strength of STAs connected to the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Displays the average signal strength of STAs connected to a specified AP radio.	The value is an integer that ranges from 0 to 2.

 Copyright © Huawei Technologies Co., Ltd.

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 14-22 Description of the **display ap sta-signal strength** command output

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

14.1.88 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.
ssid *ssid*	Specifies the SSID that STAs associate with.	The value must be an existing SSID.

 Copyright © Huawei Technologies Co., Ltd.

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 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 14-23 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 received bytes.
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 transmitted bytes.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 signal strength(dBm)(RX)                       :-
Wireless power(dBm)(RX)                                :-
Wireless unicast frames(RX)                           :30
Wireless management frames(RX)                             :506379
Wireless control frames(RX)                            :0
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 control frames(TX)                            :0
Wireless data frames(TX)                               :0
Wireless noise(dBm)                                 :-100
Wireless port up rate(Kbps)                           :40
Wireless port down rate(Kbps)                          :1
Wireless port drop rate(%)                            :42
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 DisAuth Frames                           :0
Wireless retry frames                             :515
Wireless PER(%)                                   :0
Wireless PER of the last statistic period(%)             :7
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
-------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-24 Description of the **display ap traffic statistics wireless ap-name** *ap-name* **radio** *radio-id* command output

Item	Description
Wireless frames(RX)	Number of frames received by the radio.
Wireless bytes(RX)	Number of bytes received by the radio.
Wireless error frames(RX)	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 signal strength(dBm)(RX)	Strength of signals received by the radio.
Wireless power(dBm)(RX)	Receive optical power of the radio.
Wireless unicast frames(RX)	Number of unicast frames received by the radio.
Wireless management frames(RX)	Number of management frames received on the radio.
Wireless control frames(RX)	Number of control frames received on the radio.
Wireless data frames(RX)	Number of data frames received on 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)	Number of transmitted bytes received by the radio.
Wireless RTS successes(TX)	Number of Request to Send (RTS) frames that are successfully sent by the radio.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 control frames(TX)	Number of control 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 on the radio, kbit/s.
Wireless port down rate(Kbps)	Downstream rate on the radio, kbit/s.
Wireless port drop rate(%)	Packet loss ratio on the radio, in percentage (%).
Wireless port PS-Poll Frames	Number of data frames sent by the STA working in power saving mode.
Wireless port Association Request	Number of Association Request frames.
Wireless port Association Response	Number of Association Response frames.
Wireless port ReAssociation Request	Number of Reassociation Request frames.
Wireless port ReAssociation Response	Number of Reassociation Response frames.
Wireless port Disassociation Frames	Number of Disassociation frames.
Wireless port DisAuth 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 statistic period(%)	Packet error rate in the last statistical period.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Wireless channel utilization(%)	Channel usage on the radio. **NOTE** When the working mode of an AP radio is the 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.

14.1.89 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

 Copyright © Huawei Technologies Co., Ltd.

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 14-25 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.
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.

14.1.90 display ap uncontrol all

Function

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

 Copyright © Huawei Technologies Co., Ltd.

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 14-26 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.

 Copyright © Huawei Technologies Co., Ltd.

14.1.91 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          : ftp-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 type/AP-group update filename
 AP6010DN-AGN           : FitAP6X10XN_V200R008C00.bin
-------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-27 Description of the **display ap update configuration** command output

Item	Description
AP update mode	AP upgrade mode. • FTP-mode: indicates the FTP mode. • SFTP-mode: indicates the SFTP mode. To configure the parameter, run the **14.1.21 ap update mode** command.
FTP configuration	FTP server configuration.
FTP IP	IP address of the FTP server. To configure the parameter, run the **14.1.18 ap update ftp-server** command.
FTP username	User name for logging in to the FTP server. To configure the parameter, run the **14.1.18 ap update ftp-server** command.
FTP password	Password for logging in to the FTP server. To configure the parameter, run the **14.1.18 ap update ftp-server** command.
FTP max number	Maximum number of APs that can be upgraded simultaneously in FTP mode. To configure the parameter, run the **14.1.18 ap update ftp-server** command.
SFTP configuration	SFTP server configuration.
SFTP IP	IP address of the SFTP server. To configure the parameter, run the **14.1.25 ap update sftp-server** command.
SFTP username	User name for logging in to the SFTP server. To configure the parameter, run the **14.1.25 ap update sftp-server** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SFTP password	Password for logging in to the SFTP server. To configure the parameter, run the **14.1.25 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 **14.1.25 ap update sftp-server** 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 **14.1.27 ap update update-filename** command.

14.1.92 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* }

Parameters

Parameter	Description	Value
all	Displays upgrade progress of all APs.	-
downloading	Displays APs that are upgrading.	-
failed	Displays APs that failed to be upgraded.	-
succeed	Displays APs that have been successfully upgraded.	-
ap-name *ap-name*	Displays upgrade progress of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays upgrade progress of the AP with a specified ID.	The AP ID must exist.

Copyright © Huawei Technologies Co., Ltd.

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
--------------------------------------------------------------------------------
ID   Name   Type              AP MAC         Update Status
--------------------------------------------------------------------------------
0    hw0    AP6010DN-AGN      60de-4476-e320  succeed
1    hw1    AP6010DN-AGN      60de-4476-e340  downloading(progress: 80%/0%)
2    hw2    AP6010DN-AGN      60de-4476-e360  downloading(progress: 100%/50%)
3    hw3    AP6010DN-AGN      60de-4476-e380  -
4    hw4    AP6010DN-AGN      60de-4476-e3a0  -
5    hw5    AP6010DN-AGN      60de-4476-e3c0  -
--------------------------------------------------------------------------------
Total: 6
```

Table 14-28 Description of the **display ap update status all** command

Item	Description
ID	AP ID.
Name	AP name.
Type	AP type.
AP MAC	MAC address of the AP.

 Copyright © Huawei Technologies Co., Ltd.

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 RRUs automatically upgrade at the same time, this message may also be displayed. In this situation, the actual RRU 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(analyze the version by upgrade filename): The upgrade failed because the device failed to analyze the version number in the file name. • 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. • failed(AP wait file timeout): The upgrade failed because the time that the AP waits for fragment data expired.

 Copyright © Huawei Technologies Co., Ltd.

	• failed(can not get AP type): The upgrade failed because the AC failed to obtain the AP type. • failed(change to standby): The upgrade failed due a revertive switchover failure. • failed(cut upgrade filename): The upgrade failed because the AC failed to process the upgrade file name. • 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 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(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.

 Copyright © Huawei Technologies Co., Ltd.

	• 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(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(unknown error): The upgrade failed due to an unknown error. • failed(upgrade configuration response error): The upgrade failed because there was an error in the AP's upgrade response. • failed(upgrade timeout): The upgrade timed out and failed. • failed(user canceled): The upgrade failed because the user cancels 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(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(no need to update): The upgrade succeeded. There is no need to upgrade the AP. • -: The AP requires no upgrade.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.20 ap update load
14.1.22 ap update multi-load

14.1.93 display ap username

Function

The **display ap username** command displays the user name for logging in to an AP.

Format

display ap username [**ap-name** *ap-name* | **ap-id** *ap-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the user name for logging in to the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the user name for logging in to the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ap username ap-name** *ap-name* command displays the user name for logging in to a specified AP.

Example

Display the user name for logging in to AP **huawei**.

```
<Huawei> display ap username ap-name huawei
------------------------------------------------------------------------------
AP username: admin
AP password: ******
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-29 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 **14.1.28 ap username** command.
AP password	Password for logging in to the AP. To configure the parameter, run the **14.1.28 ap username** command.

Related Topics

14.1.28 ap username

14.1.94 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.	-
ap-group *ap-group-name*	Displays version information about all APs of a specified AP group.	The AP group must exist.
version-name *version-name*	Displays version information about a specified AP.	The value is string of 11 to 17 characters, in the format of **VxxxRxxxCxxx** or **VxxxRxxxCxxxSPCxxx**. For example, V200R006C00 or V200R005C10SPC200.

Copyright © Huawei Technologies Co., Ltd.

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 : V200R010
--------------------------------------------------------------------------------
ID   Name           Group   Type           Version            state
--------------------------------------------------------------------------------
0    60de-4476-e360 default AP6010DN-AGN    V200R007C00        normal
1    1047-80b1-56a0 default AP6310SN-GN     V200R007C00        normal
2    Huawei         default AP7030DE        V200R007C00        normal
3    AP4            gjg1                    _                  idle
4    48f8-dbc9-4a40 default AP4050DE-M-S    V200R010C00SPC500  normal
--------------------------------------------------------------------------------
Total: 5, printed: 5
```

Table 14-30 Description of the **display ap version** command output

Item	Description
Compatible version	Compatible version. Only the latest compatible version of the AP is displayed.
ID	AP ID.
Name	AP name.
Group	AP group name.
Type	AP type.
Version	AP version name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
state	State of an AP. • commit-failed: WLAN service configuration commitment fails. • committing: WLAN service configuration is being committed. • config: The AP is initializing configuration. • config-failed: The AP fails to initialize the configuration. • download: The AP is downloading the upgrade software. • fault: The AP is faulty. • idle: The AP is in idle state. • name-conflicted: APs' names conflict. • nor: The AP is in normal state. • standby: The AP is on the standby AC. • ver-mismatch: Versions of the AP and AC do not match.

14.1.95 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

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

When the AP authentication mode is set to MAC authentication or SN authentication using the **14.1.11 ap auth-mode** command, you can run the **14.1.29 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 14-31 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 14-32 Description of the **display ap whitelist sn** command output

Item	Description
Index	Index.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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

14.1.29 ap whitelist

14.1.96 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.

 Copyright © Huawei Technologies Co., Ltd.

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
Wired port IPv4 inbound ACL number : -
Wired port IPv4 outbound ACL number: -
------------------------------------------------------------------------------
```

Table 14-33 Description about the **display ap wired-port gigabitethernet 0 ap-name huawei** 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

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                       : -
Wired port IPv4 Inbound ACL Number  : -
Wired port IPv4 Outbound ACL Number : -
------------------------------------------------------------------------------
```

Table 14-34 Description about the **display ap wired-port eth-trunk 0 ap-name huawei** command output

Item	Description
Eth-trunk ID	ID of the Eth-trunk interface.
Eth-trunk description	Description of the Eth-trunk interface.
STP	Whether to enable STP on the Eth-trunk interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.

14.1.97 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

 Copyright © Huawei Technologies Co., Ltd.

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 14-35 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 of the AP group **default**.

```
<Huawei> display ap-group name default
------------------------------------------------------------------------------
AP system profile          : default
Regulatory domain profile  : default
WIDS profile               : default
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
```

 Copyright © Huawei Technologies Co., Ltd.

```
 Interface GE25           : default
 Interface GE26           : default
 Interface GE27           : default
 Interface Eth-trunk0     : default
Radio 0
 Radio 2.4G profile       : default
 Radio 5G profile         : default
 VAP profile              :
 WDS profile              : default
 WDS whitelist profile    :
 Radio switch             : enable
 Channel                  : -
 Channel bandwidth        : 20mhz
 EIRP(dBm)                : 127
 Antenna gain(dB)         : -
 Coverage distance(100 m) : 3
 Radio frequency          : 2.4G
 WIDS attack detect       : -
Radio 1
 Radio 5G profile         : default
 VAP profile              :
 WDS profile              :
 WDS whitelist profile    :
 Radio switch             : enable
 Channel                  : -
 Channel bandwidth        : 20mhz
 EIRP(dBm)                : 127
 Antenna gain(dB)         : -
 Coverage distance(100 m) : 3
 Radio frequency          : 5G
 WIDS attack detect       : -
Radio 2
 Radio 5G profile         : default
 VAP profile              :
  WLAN  1                 : default
 WDS profile              :
 WDS whitelist profile    :
 Radio switch             : enable
 Channel                  : -
 Channel bandwidth        : 20mhz
 EIRP(dBm)                : 127
 Antenna gain(dB)         : -
 Coverage distance(100 m) : 3
 Radio frequency          : 5G
 WIDS attack detect       : -
```

Table 14-36 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 **14.1.42 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 **14.1.193 regulatory-domain-profile** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
WIDS profile	WIDS profile referenced by an AP group. To configure the parameter, run the **14.4.57 wids-profile (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 **14.1.241 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 **14.1.185 radio-2g-profile** command.
Radio 5G profile	5G radio profile referenced by an AP group. To configure the parameter, run the **14.1.187 radio-5g-profile** command.
VAP profile	VAP profile referenced by an AP group. To configure the parameter, run the **14.1.234 vap-profile** command.
WDS profile	WDS profile referenced by an AP group. To configure the parameter, run the **14.5.21 wds-profile radio** command.
WDS whitelist profile	WDS whitelist profile referenced by an AP group. To configure the parameter, run the **14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)** command.
Radio switch	Whether a radio is enabled. To configure the parameter, run the **14.1.183 radio disable** command.
Channel	Working channel of a radio. To configure the parameter, run the **14.1.57 channel** command.
Channel bandwidth	Operating bandwidth of a radio. To configure the parameter, run the **14.1.57 channel** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
EIRP(dBm)	Transmit power of a radio, in dBm. To configure the parameter, run the **14.1.140 eirp** command.
Antenna gain(dB)	Antenna gain of a radio, in dBm. To configure the parameter, run the **14.1.7 antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter (unit: 100 m). To configure the parameter, run the **14.1.62 coverage distance** command.
Radio frequency	Working frequency of a radio. To configure the parameter, run the **14.1.143 frequency** command.
WIDS attack detect	Whether attack detection is enabled. To configure the parameter, run the **14.4.55 wids attack detect enable** command.

Related Topics

14.1.31 ap-group

14.1.98 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.

Copyright © Huawei Technologies Co., Ltd.

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 14-37 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       : -
AP management VLAN          : -
Temporary management switch  : disable
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 high temperature threshold(degree C): -
AP low temperature threshold(degree C): -
AP CPU usage threshold(%)   : 90
AP memory usage threshold(%)  : 80
```

 Copyright © Huawei Technologies Co., Ltd.

```
Alarm restriction            : enable
Alarm restriction period(s)  : 60
Log server IP address        : -
Ethernet port MTU(byte)      : 1500
Telnet                       : enable
STelnet server               : enable
SFTP server                  : enable
Console                      : enable
Led                          : on
Report disassoc request      : enable
Dynamic blacklist aging time(s): 600
------------------------------------------------------------------------------
```

Table 14-38 Description of the **display ap-system-profile name** *profile-name* command output

Item	Description
AC priority	AC priority. To configure the parameter, run the **14.6.7 priority** command.
Protect AC IP address	IP address of the standby AC. To configure the parameter, run the **14.6.8 protect-ac** command.
AP management VLAN	Management VLAN of an AP. To configure the parameter, run the **14.1.169 management-vlan** command.
Temporary management switch	Status of management VAP and antenna alignment VAP for offline APs. To configure the parameter, run the **14.1.220 temporary-management enable (AP system profile view)** command.
STA access mode	STA access mode. To configure the parameter, run the **14.4.38 sta-access-mode** command.
STA whitelist profile	Name of a STA whitelist profile referenced by an AP system profile. To configure the parameter, run the **14.4.38 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 **14.4.38 sta-access-mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
EAPOL start mode	Eapol-start packet encapsulation mode. To configure the parameter, run the **14.1.139 eapol-start dest-address transform-to** command.
EAPOL start transform	Eapol-start packet conversion mode. To configure the parameter, run the **14.1.138 eapol-start dest-address transform-condition** command.
EAPOL response mode	Eapol-response packet encapsulation mode. To configure the parameter, run the **14.1.137 eapol-response dest-address transform-to** command.
EAPOL response transform	Eapol-response packet conversion mode. To configure the parameter, run the **14.1.136 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 **14.1.161 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 **14.1.162 lldp message-transmission hold-multiplier (AP system profile view)** command.
AP LLDP message transmission interval time(s)	Interval at which an AP sends LLDP packets to neighbors. To configure the parameter, run the **14.1.163 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 **14.1.165 lldp restart-delay** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **14.1.159 lldp admin-status** command.
AP LLDP report interval time(s)	Interval at which an AP reports LLDP neighbor information to an AC. To configure the parameter, run the **14.1.164 lldp report-interval** command.
AP high temperature threshold(degree C)	High temperature alarm threshold of an AP. To configure the parameter, run the **14.1.145 high-temperature threshold** command.
AP low temperature threshold(degree C)	Low temperature alarm threshold of an AP. To configure the parameter, run the **14.1.168 low-temperature threshold** command.
AP CPU usage threshold(%)	CPU usage alarm threshold of an AP. To configure the parameter, run the **14.1.63 cpu-usage threshold** command.
AP memory usage threshold(%)	Memory usage alarm threshold of an AP. To configure the parameter, run the **14.1.171 memory-usage threshold** command.
Alarm restriction	Alarm suppression status of an AP. To configure the parameter, run the **14.1.5 alarm-restriction disable** command.
Alarm restriction period(s)	Alarm suppression period of an AP. To configure the parameter, run the **14.1.6 alarm-restriction period** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Log server IP address	IP address of the log server. To configure the parameter, run the **14.1.167 log-server** command.
Ethernet port MTU(byte)	MTU of Ethernet interfaces. To configure the parameter, run the **14.1.172 mtu** command.
Telnet	Whether AP Telnet login is enabled. To configure the parameter, run the **14.1.219 telnet enable** command.
STelnet server	STelnet server status of an AP. To configure the parameter, run the **14.1.218 stelnet server disable** command.
SFTP server	SFTP server status of an AP. To configure the parameter, run the **14.1.210 sftp server disable** command.
Console	Whether AP console port login is enabled. To configure the parameter, run the **14.1.60 console disable** command.
Led	Whether AP indicators are allowed to turn on. • on: The AP indicators are allowed to turn on. • off: The AP indicators are forbidden to turn on. To configure the parameter, run the **14.1.157 led off** command.
Report disassoc request	Whether an AP is enabled to report disassociation request packets of STAs to the AC. To configure the parameter, run the **14.1.194 report-disassoc-request disable** command.
Dynamic blacklist aging time(s)	Aging time of a dynamic blacklist entry. To configure the parameter, run the **14.4.22 dynamic-blacklist aging-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.41 ap-system-profile (WLAN view)

14.1.99 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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
56    AP6050DN
57    AP6150DN
58    AP7050DE
59    AP7050DN-E
60    AP4030TN
61    AP4050DN-E
62    AP4050DN-HD
64    AP430-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
85    AP1050DN-S
86    AP4051TN
87    AP6052DN
88    AP7052DN
89    AP7052DE
90    AP3050DE
91    AP7152DN
92    AP8050TN-HD
93    AP8082DN
94    AP8182DN
97    AP2051DN
98    AP2051DN-S
99    AP2051DN-E
100   AP7060DN
101   AP5050DN-S
102   AP2030DN-S
103   AP4050DE-M
104   AP4050DE-M-S
105   AP100EC
106   AP200EC
107   AP300EC
108   WA375DD-CE
109   AP4050DE-B-S
110   AP5510-W-GP
111   AP2051DN-L-S
-------------------------------------------------------------------------------
Total: 74
```

NOTE

APs with the IDs of 90, 100, and 103 to 111 are supported only in the V200R010C00SPC600 version.

Table 14-39 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
Radio 1 type                      : 802.11an
  Maximal spatial streams             : 2
  Maximal antenna number              : 2
  Maximal VAP number                : 16
  Antenna gain                    : 5
Maximum station number                  : 128
AP high temperature threshold(degree C): 102
AP low temperature threshold(degree C) : -13
Outdoor                           : N
--------------------------------------------------------------------------------
```

Table 14-40 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Maximal VAP number	Maximum number of VAPs of the radio.
Antenna gain	Antenna gain of the radio, in dB.
Maximum station number	Maximum number of STAs supported by the AP type.
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.

14.1.100 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display capwap configuration
-------------------------------------------------------------
Source interface                    : -
Source ip-address                   : -
Echo interval(seconds)              : 25
Echo times                          : 6
Control priority(server to client)  : 7
Control priority(client to server)  : 7
Control-link DTLS encrypt           : enable
DTLS PSK value                      : ******
PSK mandatroy match switch          : disable
IPv6 status                         : disable
-------------------------------------------------------------
```

Table 14-41 Description of the **display capwap configuration** command output

Item	Description
Source interface	AC's source interface. To configure the parameter, run the **capwap source interface** command.
Source ip-address	IP address of the AC's source interface.
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 APs or AC receive no response from each other after the Keepalive packets are sent for the specified number of times, the APs or AC 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Control-link DTLS encrypt	Whether CAPWAP control tunnel using DTLS is enabled. To enable CAPWAP control tunnel using DTLS, run the **capwap dtls control-link encrypt** command.
DTLS PSK value	Pre-shared key for DTLS encryption. To configure the pre-shared key for DTLS encryption, run the **capwap dtls psk** command.
PSK mandatroy match switch	Whether an AP is enabled to perform DTLS sessions with the AC using the default pre-shared key. To enable an AP to perform DTLS sessions with the AC using the default pre-shared key, run the **capwap dtls psk-mandatory-match enable** command.
IPv6 status	Whether the CAPWAP tunnel supports the IPv6 function. To configure this parameter, run the **capwap ipv6 enable** command.

Related Topics

14.1.47 capwap control-link-priority
14.1.48 capwap dtls control-link encrypt
14.1.49 capwap dtls psk
14.1.50 capwap dtls psk-mandatory-match enable
14.1.51 capwap echo

14.1.101 display channel switch-record

Function

The **display channel switch-record** command displays channel switching records on the device.

Format

display channel switch-record { **all** | **ap-name** *ap-name* **radio** *radio-id* | **ap-id** *ap-id* **radio** *radio-id* | **reason** *reason* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
all	Displays all channel switching records.	-
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 • 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.

Example

Display all channel switching records.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display channel switch-record all
Old/New: Old channel/New channel
RfID   : Radio ID
------------------------------------------------------------------------------
AP name  RfID     Old/New  Switch reason  Switch time
------------------------------------------------------------------------------
L2-4f    0        1/6      wds            11:03:30 2014/9/28
------------------------------------------------------------------------------
Total : 1, printed : 1
```

Table 14-42 Description of the **display channel switch-record** command output

Item	Description
AP name	Name of an AP where channel switching has occurred.
RfID	Radio ID.
Old/New	Channels used before and after switching.
Switch reason	Reason for channel switching.
Switch time	Time when channel switch occurred.

Related Topics

14.1.198 reset channel switch-record

14.1.102 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 14-43 Description of the **display mac-address** *mac-address* **ap-all** command output

Item	Description
MAC Address	MAC address.
VLAN/VSI	VLAN or VSI to which the device belongs.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry.
AP ID	AP ID.

 Copyright © Huawei Technologies Co., Ltd.

14.1.103 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.
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.	Currently, only Ethernet interfaces are supported.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 14-44 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

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

14.1.104 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.

Copyright © Huawei Technologies Co., Ltd.

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 14-45 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
CRC error alarm           : disable
CRC error high threshold(%): 50
CRC error Low threshold(%) : 20
Shutdown switch           : disable
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-46 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 **14.1.160 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 **14.1.166 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 **14.1.166 lldp tlv-enable (AP wired port link profile view)** command.
System capability	Whether an AP's wired interface is allowed to advertise the System-capability TLV. To configure the parameter, run the **14.1.166 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 **14.1.166 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 **14.1.166 lldp tlv-enable (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 **14.1.64 crc-alarm enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CRC error high threshold(%)	Alarm threshold for CRC errors on an AP's wired interface. To configure the parameter, run the **14.1.64 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 **14.1.64 crc-alarm enable** command.
Shutdown switch	Whether the AP's wired interface function is disabled. To configure the parameter, run the **14.1.212 shutdown (AP wired port link profile view)** command.

Related Topics

14.1.64 crc-alarm enable
14.1.160 lldp enable
14.1.166 lldp tlv-enable (AP wired port link profile view)
14.1.174 port-link-profile (WLAN view)

14.1.105 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.

Copyright © Huawei Technologies Co., Ltd.

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
------------------------------------------------------------------------
AP ID Name    RfID  Band  Type    ST  CH/BW        CE/ME   STA    CU
------------------------------------------------------------------------
0     L1_003  0     2.4G  bgn     on  6/20M        27/27   0      71%
0     L1_003  1     5G    an      on  149/20M      28/28   0      39%
------------------------------------------------------------------------
Total:2
```

Table 14-47 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.
ST	Working status of an AP radio.
CH/BW	Channel/Bandwidth of an AP radio.
CE/ME	Current power of an AP radio/ Maximum power of an AP radio.
STA	Number of STAs connected to an AP radio.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
CU	Channel usage. **NOTE** When the working mode of an AP radio is the monitor mode, this parameter is displayed as -.

14.1.106 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 the **display radio-2g-profile** 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
-------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

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

Table 14-48 Description of the **display radio-2g-profile all** command output

Item	Description
Profile name	Name of a 2G radio profile.
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(ms)                 : 100
Support short preamble              : support
Channel switch announcement         : enable
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
Wifi-light mode                     : signal-strength
Utmost power switch                 : enable
Rrm-profile                         : default
Air-scan-profile                    : default
------------------------------------------------------------------
AP EDCA parameters:
-----------------------------------------------------
      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
-----------------------------------------------------
```

Table 14-49 Description of the **display radio-2g-profile name** command output

Item	Description
Radio type	Radio type. To configure the parameter, run the **14.1.188 radio-type (2G radio profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure the parameter, run the **14.2.33 power auto-adjust enable** command.
Beacon interval(ms)	Interval at which an AP sends Beacon frames, in ms. To configure the parameter, run the **14.1.46 beacon-interval** command.
Support short preamble	Whether the short preamble is supported. To configure the parameter, run the **14.1.211 short-preamble disable** command.
Channel switch announcement	Whether channel switch announcement is enabled. To configure the parameter, run the **14.1.58 channel-switch announcement disable** command.
Guard interval mode	GI mode. To configure the parameter, run the **14.1.144 guard-interval-mode** command.
HT A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure the parameter, run the **14.1.146 ht a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure the parameter, run the **14.1.147 ht a-mpdu max-length-exponent** command.
RTS-CTS-mode	RTS/CTS mode. To configure the parameter, run the **14.1.206 rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure the parameter, run the **14.1.207 rts-cts-threshold** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
802.11bg basic rate	802.11bg basic rate set. To configure the parameter, run the **14.1.133 dot11bg basic-rate** command.
802.11bg support rate	802.11bg supported rate set. To configure the parameter, run the **14.1.134 dot11bg supported-rate** command.
Multicast rate 2.4G	Multicast rate of wireless packets on the 2.4GHz radio. To configure the parameter, run the **14.1.173 multicast-rate** command.
Interference detect switch	Whether interference detection is enabled. To configure the parameter, run the **14.2.30 interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure the parameter, run the **14.2.29 interference co-channel threshold** command.
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure the parameter, run the **14.2.28 interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure the parameter, run the **14.2.31 interference station threshold** command.
WMM switch	Whether the WMM function is enabled. To configure the parameter, run the **14.1.243 wmm disable** command.
Mandatory switch	Whether to allow STAs that do not support WMM to connect to a WMM-enabled AP. To configure the parameter, run the **14.1.246 wmm mandatory enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Wifi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure the parameter, run the **14.1.239 wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure the parameter, run the **14.2.36 rrm-profile (radio profile view)** command.
Air-scan-profile	Name of the air scan profile referenced by a radio profile. To configure the parameter, run the **14.2.3 air-scan-profile (radio profile view)** command.
Utmost power switch	Whether a radio is enabled to send packets at maximum power. To configure the parameter, run the **14.1.232 utmost-power disable** command.
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VO	AC_VO packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VI	AC_VI packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BE	AC_BE packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BK	AC_BK packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
TXOPLimit	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which an STA can occupy a channel. A larger value indicates a longer duration. To configure the parameter, run the **14.1.244 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 the parameter, run the **14.1.244 wmm edca-ap** command.

14.1.107 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* }

Copyright © Huawei Technologies Co., Ltd.

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 the **display radio-5g-profile** 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 14-50 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(ms)                 : 100
Beamforming switch                  : disable
Support short preamble              : not support
Channel switch announcement         : support
Guard interval mode                 : normal
```

 Copyright © Huawei Technologies Co., Ltd.

```
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
------------------------------------------------------------
AP EDCA parameters:
-----------------------------------------------------
      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
-----------------------------------------------------
```

Table 14-51 Description of the **display radio-5g-profile name** command output

Item	Description
Radio type	Radio type. To configure the parameter, run the **14.1.189 radio-type (5G radio profile view)** command.
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure the parameter, run the **14.2.33 power auto-adjust enable** command.
Beacon interval(ms)	Interval at which an AP sends Beacon frames, in ms. To configure the parameter, run the **14.1.46 beacon-interval** command.
Beamforming switch	Whether the beamforming function is enabled. When the WLAN mode is AC, this parameter cannot be set.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Support short preamble	Whether the short preamble is supported. To configure the parameter, run the **14.1.211 short-preamble disable** command.
Channel switch announcement	Whether channel switch announcement is enabled. To configure the parameter, run the **14.1.58 channel-switch announcement disable** command.
Guard interval mode	GI mode. To configure the parameter, run the **14.1.144 guard-interval-mode** command.
HT A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure the parameter, run the **14.1.146 ht a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure the parameter, run the **14.1.147 ht a-mpdu max-length-exponent** command.
VHT A-MPDU length limit	Maximum length of the frame aggregated in A-MSDU mode. To configure the parameter, run the **14.1.235 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 the parameter, run the **14.1.236 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 the parameter, run the **14.1.237 vht a-msdu max-frame-num** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RTS-CTS-mode	RTS/CTS mode. To configure the parameter, run the **14.1.206 rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure the parameter, run the **14.1.207 rts-cts-threshold** command.
802.11a basic rate	802.11a basic rate set. To configure the parameter, run the **14.1.131 dot11a basic-rate** command.
802.11a support rate	802.11a supported rate set. To configure the parameter, run the **14.1.132 dot11a supported-rate** command.
Multicast rate 5G	Multicast rate of wireless packets on the 5 GHz radio. To configure the parameter, run the **14.1.173 multicast-rate** command.
VHT mcs	Maximum MCS value corresponding to a specific number of 802.11ac spatial streams. To configure the parameter, run the **14.1.238 vht mcs-map** command.
Interference detect switch	Whether interference detection is enabled. To configure the parameter, run the **14.2.30 interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure the parameter, run the **14.2.29 interference co-channel threshold** command.
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure the parameter, run the **14.2.28 interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure the parameter, run the **14.2.31 interference station threshold** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
WMM switch	Whether the WMM function is enabled. To configure the parameter, run the **14.1.243 wmm disable** command.
Mandatory switch	Whether to allow STAs that do not support WMM to connect to a WMM-enabled AP. To configure the parameter, run the **14.1.246 wmm mandatory enable** command.
Auto-off start time	Start time for scheduled VAP auto-off.
Auto-off end time	End time for scheduled VAP auto-off.
WiFi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure the parameter, run the **14.1.239 wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure the parameter, run the **14.2.36 rrm-profile (radio profile view)** command.
Air-scan-profile	Name of the air scan profile referenced by a radio profile. To configure the parameter, run the **14.2.3 air-scan-profile (radio profile view)** command.
Utmost power switch	Whether a radio is enabled to send packets at maximum power. To configure the parameter, run the **14.1.232 utmost-power disable** command.
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VO	AC_VO packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VI	AC_VI packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AC_BE	AC_BE packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BK	AC_BK packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
TXOPLimit	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which an STA can occupy a channel. A larger value indicates a longer duration. To configure the parameter, run the **14.1.244 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 the parameter, run the **14.1.244 wmm edca-ap** command.

 Copyright © Huawei Technologies Co., Ltd.

14.1.108 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 14-52 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.

 Copyright © Huawei Technologies Co., Ltd.

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

14.1.109 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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-53 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.

14.1.110 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
------------------------------------------------------------------
AP-group                    ap-group1
```

 Copyright © Huawei Technologies Co., Ltd.

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

Table 14-54 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.

14.1.111 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
------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
Reference type              Reference name
------------------------------------------------------------------------
AP-group                    ap-group1
------------------------------------------------------------------------
Total:1
```

Table 14-55 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.

14.1.112 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.

 Copyright © Huawei Technologies Co., Ltd.

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 14-56 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.

14.1.113 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

 Copyright © Huawei Technologies Co., Ltd.

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 14-57 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.

14.1.114 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

 Copyright © Huawei Technologies Co., Ltd.

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 14-58 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.

14.1.115 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.

 Copyright © Huawei Technologies Co., Ltd.

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 14-59 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.

14.1.116 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*

 Copyright © Huawei Technologies Co., Ltd.

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           huawei                         Ethernet0
------------------------------------------------------------------------------
Total: 1
```

Table 14-60 Description of the **display references wired-port-profile** command output

Item	Description
Reference type	Type of the profile by which an AP wired port profile is referenced.
Reference name	Name of the profile by which an AP wired port profile is referenced.
Reference port	Interface by which an AP wired port profile is referenced.

14.1.117 display regulatory-domain-profile

Function

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

 Copyright © Huawei Technologies Co., Ltd.

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 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 14-61 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
------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
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
-------------------------------------------------------------
```

Table 14-62 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 **14.1.61 country-code** command.
2.4G dca channel-set	2.4G radio calibration channel set. To configure the parameter, run the **14.2.16 dca-channel channel-set** command.
5G dca bandwidth	5G radio calibration bandwidth. To configure the parameter, run the **14.2.15 dca-channel bandwidth** command.
5G dca channel-set	5G radio calibration channel set. To configure the parameter, run the **14.2.16 dca-channel channel-set** command.

Related Topics

14.1.61 country-code
14.2.15 dca-channel bandwidth
14.2.16 dca-channel channel-set

14.1.118 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* }

 Copyright © Huawei Technologies Co., Ltd.

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                Reference
-------------------------------------------------------------
default                     1
ssid-profile-1              0
-------------------------------------------------------------
Total: 2
```

Table 14-63 Description of the **display ssid-profile all** command output

Item	Description
Profile name	SSID profile name.
Reference	Number of times an SSID profile is referenced.

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
```

 Copyright © Huawei Technologies Co., Ltd.

```
Legacy station              : enable
DTIM interval               : 1
beacon-2g-rate              : 1
beacon-5g-rate              : 6
deny-broadcast-probe        : disable
probe-response-retry num    : 1
Active dull client          : 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 14-64 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 **14.1.214 ssid** command.
SSID hide	SSID hiding. To configure the parameter, run the **14.1.215 ssid-hide enable** command.
Association timeout(min)	Association timeout period. To configure the parameter, run the **14.1.43 association-timeout** command.
Max STA number	Maximum number of users. To configure the parameter, run the **14.1.170 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 **14.1.191 reach-max-sta hide-ssid disable** command.
Legacy station	Whether to permit access of legacy terminals. To configure the parameter, run the **14.1.158 legacy-station disable** command.
DTIM interval	DTIM interval. To configure the parameter, run the **14.1.135 dtim-interval** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
beacon-2g-rate	Rate at which 2.4 GHz Beacon frames are sent. To configure the parameter, run the **14.1.44 beacon-2g-rate** command.
beacon-5g-rate	Rate at which 5 GHz Beacon frames are sent. To configure the parameter, run the **14.1.45 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 **14.1.65 deny-broadcast-probe enable** command.
probe-response-retry num	Number of times Probe Response packets are retransmitted. To configure the parameter, run the **14.1.181 probe-response-retry** command.
Active dull client	Whether the function of preventing terminals from entering energy-saving mode is enabled. To configure the parameter, run the **14.1.4 active-dull-client enable** command.
AC_VO	AC_VO packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VI	AC_VI packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BE	AC_BE packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BK	AC_BK packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
TXOPLimit	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which an STA can occupy a channel. A larger value indicates a longer duration. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

14.1.119 display station

Function

The **display station** command displays STA access information.

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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 STA access information.

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  IPv4 address   SSID       IPv6 address
--------------------------------------------------------------------------------------------------------------------------------
84db-ac68-2017  0     area_1   0/1      2.4G  11n   64/64     -50   100   192.168.20.173 wlan-net
FE80::86DB:ACFF:FE68:2017
b863-4d02-c617  0     area_1   1/1      5G    11n   97/114    -38   100   192.168.20.31  wlan-net5g
FE80::4:F75D:620C:FA02
--------------------------------------------------------------------------------------------------------------------------------
Total: 2 2.4G: 1 5G: 1
```

Table 14-65 Description of the **display station all** command output

Item	Description
STA MAC	STA's MAC address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 a STA.
VLAN	VLAN ID of a STA.
IPv4 address	IPv4 address of a STA.
SSID	SSID name.
IPv6 address	IPv6 address of a STA.

Display access information about a specified STA.

```
<Huawei> display station sta-mac b878-2eb4-2689
--------------------------------------------------------------------------------
Station MAC-address                      : b878-2eb4-2689
Station IP-address                       : 2.2.2.1
                                         : FE80::C87:23F4:A6D:8D03
Station gateway                          : 2.2.2.2
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
  This is an ATH node                    : No
  WDS workaround req                     : No
  WDS link                               : No
  PMF negotiation                        : No
Station's HT capability                  : WQ
Station ERP element                      : 0
Station capabilities                     : E
Station PMF capabilities                 : PMFC=0,PMFR=0
Station VHT capabilities
  256QAM capabilities                    :No
  VHT Explicit Beamforming capabilities  :No
Station's RSSI(dBm)                      : -28
Station's Noise(dBm)                     : -108
Station's radio mode                     : 11n
Station's AP Name                        : area_3
```

 Copyright © Huawei Technologies Co., Ltd.

```
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                   : 7
Station's Short GI                    : nonsupport
Station's roam state                   : No
Station supported band                   : Dual Band
Station support 802.11k                : 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
-------------------------------------------
-------------------------------------------
--------------------------------------------------------------------------------
```

Table 14-66 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)	Upstream signal noise ratio of a STA, in dB.
The upstream aggregate receive power(dBm)	Upstream receive power of a STA, in dBm.
Station connect rate(Mbps)	Connection rate of a STA, in Mbit/s.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.
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.
Station ERP element	ERP of a STA, in dBm.
Station capabilities	Capabilities of a STA.
Station PMF capabilities	PMF capability of a STA.
Station VHT capabilities	VHT capability of a STA.
256QAM capabilities	Whether a STA supports 802.11ac.
VHT Explicit Beamforming capabilities	Whether a STA supports 802.11ac explicit Beamforming.
Station's RSSI(dBm)	Received signal strength indicator (RSSI) of a STA, in dBm.
Station's Noise(dBm)	Interference signal strength of a STA, in dBm.
Station's radio mode	Radio mode of a STA.
Station's AP Name	Name of the AP which a STA associates with.
Station's Radio ID	Radio ID of a STA.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Station's Authentication Method	Authentication mode of a STA.
Station's Cipher Type	Encryption mode of a STA.
Station's User Name	User name of a STA.
Station's Vlan ID	VLAN ID of a STA.
Station's Channel Band-width	Channel bandwidth of a STA.
Station's asso BSSID	BSSID 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.
Station's MCS value	MCS value of the STA.
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 802.11v	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.

14.1.120 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-67 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

14.1.200 reset station assoc-info ap-offline-record

14.1.121 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

 Copyright © Huawei Technologies Co., Ltd.

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

Displays 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 14-68 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.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reason	Reason for the STA online failure. ● A user has gone offline unexpectedly. ● STA association request error. ● Incorrect encryption mode. ● The STA needs to send an authentication request before associating with the network. ● The authentication request is not approved. ● The AP does not support the rate set specified in the association request packet of the STA. ● Incorrect encryption mode in the authentication frame. ● Failed to decrypt the challenge packet. ● The radio mode does not match. ● The number of STAs exceeds the maximum allowed by the AP. ● The terminal capability set does not match the capabilities configured for the VAP. The WMM capabilities do not match. ● The terminal capability set does not match the capabilities configured for the VAP. The network type flag carried by the terminal is incorrect. ● The terminal capability set does not match the capabilities configured for the VAP. The terminal does not support short slot time. ● The terminal capability set does not match the capabilities configured for the VAP. In the 802.11h only mode, the terminal does not support dynamic frequency selection. ● The number of associated STAs exceeds the maximum allowed by the AC. ● The STA is not in the global whitelist. ● The STA is in the global blacklist.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• The STA is not in the VAP's whitelist. • The STA is in the VAP's blacklist. • The STA is in the dynamic blacklist. • The association or reassociation packet check fails. • The number of users exceeds the maximum allowed on the VAP. • The STA uses a static IP address. • The STA's SNR is below the specified threshold. • The number of STAs of the radio has reached the upper threshold. • The channel utilization of the radio has reached the upper threshold. • The number of STAs exceeds the maximum allowed by the radio. • The number of STAs exceeds the maximum allowed in the VAP. • Failed to decrypt the challenge packet. • The key is incorrect or the STA uses the cached PMK. • Time to wait for the STA's handshake packet (2/4) expires. • Time to wait for the STA's handshake packet (4/4) expires. • WAPI authentication times out. • Authentication fails. • Reauthentication fails.

Related Topics

14.1.202 reset station online-fail-record

14.1.122 display station offline-record

Function

The **display station offline-record** command displays STA offline records.

 Copyright © Huawei Technologies Co., Ltd.

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 14-69 Description of the **display station offline-record** command output

Item	Description
STA MAC	MAC address of a STA.
AP ID	AP ID.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
Total stations	Total number of STAs.
Total records	Total number of STA offline records.

Related Topics

14.1.201 reset station offline-record

14.1.123 display station statistics

Function

The **display station statistics** command displays statistics information about STAs.

Format

display station statistics [**sta-mac** *sta-mac-address* | **ap-name** *ap-name* | **ap-id** *ap-id*]

Parameters

Parameter	Description	Value
sta-mac *sta-mac-address*	Displays statistics information about a STA with a specified MAC address.	The STA's MAC address must exist.
ap-name *ap-name*	Displays statistics information about STAs on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays statistics information about STAs on the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

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.

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 auth successful                                 :0
 AC roaming                                        :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 clients detected                           :0
 Stations supporting dual band                          :0
 Online stations                                   :0
    Stations associated with 2.4G band                     :0
    Stations associated with 5G band                       :0
------------------------------------------------------------------------------
```

Table 14-70 Description of the **display station statistics** command output

Item	Description
AC 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 roaming	Total number of times that roaming occurs on the AC.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AC auth failed because of password error	Number of STAs that fail to be authenticated due to incorrect passwords.
AC auth failed because of invalid calc	Number of STAs that fail to be authenticated due to an invalid authentication algorithm.
AC auth failed because of timeout	Number of STAs that fail to be authenticated due to timeout.
AC auth failed because of being refused	Number of STAs that fail to be authenticated because the AC rejects the associate requests.
AC auth failed because of other reasons	Number of STAs that fail to be authenticated due to other reasons.
Sticky clients detected	Number of 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.
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
 STA power save percent                             : 0%
------------------------------------------------------------------------------
```

Table 14-71 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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
 Average rate of all stations(kbps)                           :63476
 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
 Load balancing status between dual band                      :Balanced
 Detected as sticky clients                                   :0
 Online stations                                              :0
--------------------------------------------------------------------------------
```

Table 14-72 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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.
Average rate of all stations(kbps)	Average rate of all STAs, in kbit/s.
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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 GHz 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.
Load balancing status between dual band	Status of load balancing between the 2.4 GHz and 5 GHz frequency bands.
Detected as sticky clients	Number of the detected sticky terminals.
Online stations	Number of online STAs.

14.1.124 display traffic-profile

Function

The **display traffic-profile** command displays configuration information about a traffic profile.

Format

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

 Copyright © Huawei Technologies Co., Ltd.

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

The user priority of 802.11e packets is mapped to DSCP priority in the CAPWAP header when packets are sent from an AP to an 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
Traffic optimize sta bridge forward : enable
IGMP snooping               : enable
IGMP snooping report suppress : disable
Traffic optimize broadcast suppression(pps): -
Traffic optimize multicast suppression(pps): -
Traffic optimize unicast suppression(pps): -
Traffic optimize multicast to unicast: disable
Priority map 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
                                6 map 48
                                7 map 56
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
-----------------------------------------------------
```

The DSCP priority of 802.11e packets is mapped to the user priority of tunnel packets when packets are sent to APs.

```
<Huawei> display traffic-profile name p1
-----------------------------------------------------
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
Traffic optimize sta bridge forward : enable
IGMP snooping                 : enable
IGMP snooping report suppress : disable
Traffic optimize broadcast suppression(pps): -
Traffic optimize multicast suppression(pps): -
Traffic optimize unicast suppression(pps): -
Traffic optimize multicast to unicast: disable
Priority map upstream trust   : DSCP
WMM priority downstream map mode: DSCP map 802.11e
                               0-7 map 0
                               8-15 map 1
                               16-23 map 2
                               24-31 map 3
                               32-39 map 4
                               40-47 map 5
                               48-55 map 6
                               56-63 map 7
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
```

 Copyright © Huawei Technologies Co., Ltd.

```
                    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
------------------------------------------------------
```

Table 14-73 Description of the **display 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 802.11e user priority when 802.3 packets are sent to an AP from upper-layer devices. To configure the parameter, run the **14.1.177 priority-map downstream trust** command.
User isolate mode	User isolation. To configure the parameter, run the **14.5.14 user-isolate (traffic profile view)** command.
Rate limit client up(Kbps)	Indicates upstream rate limit configured for STAs. To configure the parameter, run the **14.1.190 rate-limit** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rate limit client down(Kbps)	Indicates downstream rate limit configured for STAs. To configure the parameter, run the **14.1.190 rate-limit** command.
Rate limit VAP up(Kbps)	Indicates upstream rate limit configured for VAPs. To configure the parameter, run the **14.1.190 rate-limit** command.
Rate limit VAP down(Kbps)	Indicates downstream rate limit configured for VAPs. To configure the parameter, run the **14.1.190 rate-limit** command.
Traffic optimize sta bridge forward	Function of forbidding STA bridging packet forwarding.
IGMP snooping	IGMP snooping.
IGMP snooping report suppress	IGMP message suppression time.
Traffic optimize broadcast suppression(pps)	Maximum broadcast traffic volume allowed on an interface. To configure the parameter, run the **14.1.223 traffic-optimize broadcast-suppression** command.
Traffic optimize multicast suppression(pps)	Maximum multicast traffic volume allowed on an interface. To configure the parameter, run the **14.1.224 traffic-optimize multicast-suppression** command.
Traffic optimize unicast suppression(pps)	Maximum unicast traffic volume allowed on an interface. To configure the parameter, run the **14.1.227 traffic-optimize unicast-suppression** command.
Traffic optimize multicast to unicast	Function of converting multicast packets to unicast packets. To configure the parameter, run the **14.1.225 traffic-optimize multicast-unicast enable** command.
CAPWAP priority upstream map mode	Mapping from WMM to the DSCP priority of the upstream CAPWAP tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Priority map upstream trust	Mapping from the 802.11e user priority or DSCP priority of 802.3 packets to the user priority of tunnel packets. To configure the parameter, run the **14.1.180 priority-map tunnel-upstream trust** command.
WMM priority downstream map mode	Mapping from the DSCP priority to the WMM of downstream packets.

Display configurations of all traffic profiles.

```
<Huawei> display traffic-profile all
-------------------------------------------------------
Profile name                    Reference
-------------------------------------------------------
default                          3
1                               1
p1                               0
-------------------------------------------------------
Total: 3
```

Table 14-74 Description of the **display traffic-profile all** command output

Item	Description
Profile name	Profile name. To configure the parameter, run the **14.1.229 traffic-profile (WLAN view)** command.
Reference	Number of times a location profile is referenced.

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.125 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*]

Copyright © Huawei Technologies Co., Ltd.

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.
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 14-75 Description of the **display vap** command output

Item	Description
AP ID	AP ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

14.1.126 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

 Copyright © Huawei Technologies Co., Ltd.

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  Source Name
VAP Type        Reason
--------------------------------------------------------------------------------
e468-a350-8a60  0/4      1             ap-group     default
Service         Preshared key is not configured.
e468-a350-8a60  1/4      1             ap-group     default
Service         Preshared key is not configured.
e468-a350-8a60  0/6      1             ap-group     1
Service         Preshared key is not configured.
e468-a350-8a60  1/6      1             ap-group     1
Service         Preshared key is not configured.
--------------------------------------------------------------------------------
Total records: 4
```

Table 14-76 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
Source Name	Name of the object to which the VAP is bound.
VAP Type	VAP type, including • Service: Service VAP • WDS: WDS VAP
Reason	Reason why the VAP fails to be created.

 Copyright © Huawei Technologies Co., Ltd.

14.1.127 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
------------------------------------------------------------
Profile name                Reference
------------------------------------------------------------
default                     1
vap-profile-1               0
------------------------------------------------------------
Total: 2
```

Table 14-77 Description of the **display vap-profile all** command output

Item	Description
Profile name	VAP profile name.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reference	Number of times a VAP profile is referenced.

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

```
<Huawei> display vap-profile name default
------------------------------------------------------------------------------
Type                          : service
Forward mode                  : direct-forward
Offline management            : disable
Service VLAN ID               : 1
Learn client address          : enable
Learn client DHCP strict      : disable
Learn client DHCP blacklist   : disable
IP source check               : disable
DHCP trust port               : disable
SSID profile                  : default
Security profile              : default
Traffic profile               : default
Authentication profile        :
------------------------------------------------------------------------------
```

Table 14-78 Description of the **display vap-profile name** *profile-name* command output

Item	Description
Type	VAP type. • service: indicates the service type. • ap-management: indicates the management AP type. To configure the parameter, run the **14.1.230 type (VAP profile view)** command.
Forward mode	Data forwarding mode. • direct-forward: Indicates direct forwarding. • tunnel: Indicates tunnel forwarding. To configure the parameter, run the **14.1.142 forward-mode** command.
Offline management	Whether to enable management VAP and antenna alignment VAP for offline APs. To configure the parameter, run the **14.1.221 temporary-management enable (VAP profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Service VLAN ID	Service VLAN ID. To configure the parameter, run the **14.1.208 service-vlan** command.
Learn client address	Status of STA address learning. To configure the parameter, run the **14.1.155 learn-client-address disable** command.
Learn client DHCP strict	Status of strict STA IP address learning through DHCP. To configure the parameter, run the **14.1.154 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 **14.1.154 learn-client-address dhcp-strict** command.
IP source check	Status of IP source guard. To configure the parameter, run the **14.1.150 ip source check user-bind enable** command.
DHCP trust port	Status of the DHCP trusted interface function. To configure the parameter, run the **14.1.67 dhcp trust port** command.
SSID profile	Name of the SSID profile referenced by a VAP profile. To configure the parameter, run the **14.1.217 ssid-profile (VAP profile view)** command.
Security profile	Name of the security profile referenced by a VAP profile. To configure the parameter, run the **14.4.36 security-profile (VAP profile view)** command.
Traffic profile	Name of the traffic profile referenced by a VAP profile. To configure the parameter, run the **14.1.228 traffic-profile (VAP profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication profile	Name of the authentication profile referenced by a VAP profile.

Related Topics

14.1.233 vap-profile (WLAN view)

14.1.128 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
-------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
default                    1
wired-port-profile-1       0
------------------------------------------------------------
Total: 2
```

Table 14-79 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                  :
Port work mode                : -
Port Tagged VLAN              : -
Port untagged VLAN            : 1
Port PVID VLAN                : -
User isolate mode             : disable
DHCP trust port               : enable
IPSG switch                   : disable
DAI switch                    : disable
Learn client address switch   : disable
Traffic optimize broadcast suppression(pps)    : -
Traffic optimize unicast suppression(pps)      : -
Traffic optimize multicast suppression(pps)    : -
------------------------------------------------------------------------------
```

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 14-80 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 **14.1.175 port-link-profile (AP wired port profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Description	Interface description. To configure the parameter, run the **14.1.66 description (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 **14.5.8 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 **14.5.17 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 **14.5.17 vlan (AP wired port profile view)** command.
Port PVID VLAN	PVID of a wired interface. To configure the parameter, run the **14.5.17 vlan (AP wired port profile view)** command.
User isolate mode	User isolation status on a wired interface. To configure the parameter, run the **14.5.13 user-isolate (AP wired port profile view)** command.
DHCP trust port	Status of the DHCP trusted interface function. To configure the parameter, run the **14.1.67 dhcp trust port** command.
Ethernet trunk ID	ID of the Eth-Trunk interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSG switch	Whether IP source guard (IPSG) is enabled on an AP's wired interface. To configure the parameter, run the **14.1.151 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 **14.1.68 dai enable (AP wired port profile view)** command.
Learn client address switch	Whether terminal address learning is enabled on an AP's wired interface. To configure the parameter, run the **14.1.156 learn-client-address enable (AP wired port profile view)** command.
Traffic optimize broadcast suppression(pps)	Maximum broadcast traffic volume allowed on an AP's wired interface. To configure the parameter, run the **14.1.222 traffic-optimize (AP wired port profile view)** command.
Traffic optimize unicast suppression(pps)	Maximum unknown unicast traffic volume allowed on an AP's wired interface. To configure the parameter, run the **14.1.222 traffic-optimize (AP wired port profile view)** command.
Traffic optimize multicast suppression(pps)	Maximum multicast traffic volume allowed on an AP's wired interface. To configure the parameter, run the **14.1.222 traffic-optimize (AP wired port profile view)** command.

Related Topics

14.1.240 wired-port-profile (WLAN view)

14.1.129 display wlan config-errors

Function

The **display wlan config-errors** command displays WLAN configuration errors.

Copyright © Huawei Technologies Co., Ltd.

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 14-81 Description of the **display wlan config-errors** command output

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

14.1.130 display workmode wlan

Function

The **display workmode wlan** command displays the current WLAN mode and the configured WLAN mode of a device.

Format

display workmode wlan

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check the current WLAN mode and the configured WLAN mode of a device. The configured WLAN mode takes effect after the device is restarted.

Example

Display the current WLAN mode of the device.

```
<Huawei> display workmode wlan
 Wlan Current WorkMode = ap
 Wlan Config WorkMode  = ac
```

Table 14-82 Description of the display workmode wlan command output

Item	Description
Wlan Current WorkMode	Current WLAN mode of a device. • ap: Fat AP mode • ac: AC mode
Wlan Config WorkMode	Configured WLAN mode, which takes effect after the device is restarted. • ap: Fat AP mode • ac: AC mode

Related Topics

14.1.209 set workmode wlan

14.1.131 dot11a basic-rate

Function

The **dot11a basic-rate** command configures a basic rate set of the 802.11a protocol in a 5G radio profile.

Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] dot11a basic-rate 6 9
```

Related Topics

14.1.107 display radio-5g-profile

14.1.132 dot11a supported-rate

14.1.132 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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] dot11a supported-rate 6 9
```

Related Topics

14.1.107 display radio-5g-profile

14.1.131 dot11a basic-rate

14.1.133 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

Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] dot11bg basic-rate 6 9
```

Related Topics

14.1.106 display radio-2g-profile

14.1.134 dot11bg supported-rate

14.1.134 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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] dot11bg supported-rate 6 9
```

Related Topics

14.1.106 display radio-2g-profile

14.1.133 dot11bg basic-rate

14.1.135 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

 Copyright © Huawei Technologies Co., Ltd.

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 DITM. 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 ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] dtim-interval 5
```

Related Topics

14.1.118 display ssid-profile

14.1.136 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[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

14.1.98 display ap-system-profile

14.1.137 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

- 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 ac
[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

14.1.98 display ap-system-profile

14.1.138 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.	-

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.139 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 ac
[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

14.1.98 display ap-system-profile

14.1.139 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[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

14.1.98 display ap-system-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.140 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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] eirp 30
```

Related Topics

14.1.74 display ap config-info

14.1.105 display radio

14.1.141 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

 Copyright © Huawei Technologies Co., Ltd.

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, working mode, descriptions, LLDP function, and alarm function for CRC errors.

Precautions

APs that have only one physical network interface do not support this command.

Example

Add the AP interface to Eth-Trunk 0.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wired-port1
[Huawei-wlan-wired-port-wired-port1] eth-trunk 0
```

Related Topics

14.1.128 display wired-port-profile

14.1.142 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[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
Info: This operation may take a few seconds, please wait.done.
```

Related Topics

14.1.127 display vap-profile

14.1.143 frequency

Function

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

 Copyright © Huawei Technologies Co., Ltd.

(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 work on the 5 GHz frequency band.

Format

frequency { 2.4g | 5g }

undo frequency

Parameters

Parameter	Description	Value
2.4g	Indicates that the radio works at the 2.4 GHz frequency band.	-
5g	Indicates that the radio works at the 5 GHz frequency band.	-

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Radio 0s of the AP2010DN 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 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 and AP8130DN.

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.

 Copyright © Huawei Technologies Co., Ltd.

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

Example

Set the working frequency to the 5 GHz frequency band for radio 0 of AP 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] frequency 5g
```

Related Topics

14.1.98 display ap-system-profile

14.1.144 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 normal.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] guard-interval-mode short
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.145 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 14-83 Default upper temperature alarm threshold for APs

AP Model	Default Value (°C)
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
AP7110SN	76
AP7110DN	89
AP7030DE/AP8030DN/AP8130DN/ AP9330DN	83
AP9131DN	84

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AP2010DN, AP2030DN, AP3010DN-AGN, AP5010SN-GN, AP5010DN-AGN, AP4030DN 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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] high-temperature threshold 65
```

Related Topics

14.1.98 display ap-system-profile

14.1.146 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] ht a-mpdu disable
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.147 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] ht a-mpdu max-length-exponent 2
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.148 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

 Copyright © Huawei Technologies Co., Ltd.

A traffic profile has been created.

Example

Enable IGMP snooping in traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] igmp-snooping enable
```

14.1.149 igmp-snooping report-suppress

Function

The **igmp-snooping report-suppress** command configures IGMP Report message suppression 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

 Copyright © Huawei Technologies Co., Ltd.

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 IGMP Report message suppression in traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[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

10.9.1 display igmp-snooping

14.1.148 igmp-snooping enable (traffic profile view)

10.9.17 igmp-snooping querier enable

10.9.31 igmp-snooping suppress-time

14.1.150 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] ip source check user-bind enable
```

Related Topics

14.1.127 display vap-profile

14.4.15 display station dynamic-blacklist

14.1.155 learn-client-address disable

14.1.151 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

ipsg enable

undo ipsg enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attackers often use packets with the source IP addresses or MAC addresses of authorized users to access or attack networks. As a result, authorized users cannot obtain stable and secure network services. You can enable the IPSG function to prevent the situation.

Prerequisites

Terminal address learning has been enabled on the AP's wired interface using the **learn-client-address enable** command.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

This command takes effect only on IP packets transmitted on an AP's wired interface.

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 ac
[Huawei-wlan-view] wired-port-profile name wire1
[Huawei-wlan-wired-port-wire1] ipsg enable
```

Related Topics

14.1.128 display wired-port-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.152 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 depends 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.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] keep-service enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.98 display ap-system-profile

14.1.153 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

undo keep-service enable

Parameters

None

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

The security policy used by the APs must be WEP or WPA/WPA2-PSK.

Precautions

The command does not take effect on a WDS network.

Example

Enable the APs in fault state to allow access of new STAs.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] keep-service enable allow new-access
Info: This configuration is invalid for the WDS network.
```

14.1.154 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.

 Copyright © Huawei Technologies Co., Ltd.

If **blacklist enable** is not specified, the STA can associate with the AP but the AP does not learn the IP address of the STA.

Prerequisites

STA address learning has been enabled using the **undo learn-client-address disable** command.

Precautions

After strict STA IP address learning is enabled, it is recommended that you run the **14.1.150 ip source check user-bind enable** commands to enable IP source guard 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 ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] learn-client-address dhcp-strict
```

Related Topics

14.1.127 display vap-profile

14.1.150 ip source check user-bind enable

14.1.155 learn-client-address disable

Function

The **learn-client-address disable** command disables STA address learning.

The **undo learn-client-address disable** command enables STA address learning.

By default, STA address learning is enabled.

Format

learn-client-address disable

undo learn-client-address disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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

Precautions

- Before disabling STA address learning, run the **undo learn-client-address dhcp-strict** command to disable strict STA IP address learning through DHCP.
- 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

Disable STA address learning.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] learn-client-address disable
```

Related Topics

14.1.127 display vap-profile

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

Function

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

The **undo learn-client-address enable** command disables terminal 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 enable

undo learn-client-address enable

Parameters

None

Views

AP wired port profile view

 Copyright © Huawei Technologies Co., Ltd.

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 IP address and MAC address binding entries of wired terminals.

Prerequisites

The DHCP trusted interface has been enabled using the **undo dhcp trust port** command in the AP wired port profile view.

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 address learning on an AP's wired interface.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wire1
[Huawei-wlan-wired-port-wire1] learn-client-address enable
```

Related Topics

14.1.128 display wired-port-profile

14.1.157 led off

Function

The **led off** command forbids AP indicators to turn on.

The **undo led off** command restores the default settings.

By default, the AP indicators are allowed to turn on.

Format

led off

 Copyright © Huawei Technologies Co., Ltd.

undo led off

Parameters

None.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent AP indicators in hospitals and hotels from affecting people's rest at night, run the **led off** command to forbid AP indicators to turn on.

If you need to locate AP faults by observing AP indicator status, run the **undo led off** command to allow the AP indicators to turn on.

Example

Forbid AP indicators to turn on.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] led off
```

Related Topics

14.1.98 display ap-system-profile

14.1.158 legacy-station disable

Function

The **legacy-station disable** command denies access of legacy terminals.

The **undo legacy-station disable** command permits access of legacy terminals.

By default, access of legacy terminals is permitted.

Format

legacy-station disable

undo legacy-station disable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Legacy terminals support only 802.11a, 802.11b, or 802.11g, and provide a rate far smaller than 802.11n and 802.11ac terminals. If the legacy terminals access the wireless network, data transmission rate of the 802.11n and 802.11ac terminals will be reduced. To prevent transmission rate of 802.11n and 802.11ac terminals from being affected, run the **legacy-station disable** command to deny access of legacy terminals.

Configuration Impact

After the **legacy-station disable** command is run, legacy terminals supporting only 802.11a, 802.11b, or 802.11g cannot access the wireless network.

Example

Deny access of legacy terminals.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] legacy-station disable
```

Related Topics

14.1.118 display ssid-profile

14.1.159 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp admin-status tx
```

Related Topics

14.1.98 display ap-system-profile

14.1.160 lldp enable

Function

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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.15 ap lldp enable** command.

Example

Enable LLDP on the AP wired interface.

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.1.15 ap lldp enable

14.1.104 display port-link-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.161 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp message-transmission delay 10
```

Related Topics

14.1.98 display ap-system-profile
14.1.163 lldp message-transmission interval (AP system profile view)

 Copyright © Huawei Technologies Co., Ltd.

14.1.162 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp message-transmission hold-multiplier 5
```

Related Topics

14.1.98 display ap-system-profile

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

14.1.163 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

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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 second.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp message-transmission interval 60
```

Related Topics

14.1.98 display ap-system-profile

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

14.1.164 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp report-interval 20
```

Related Topics

14.1.98 display ap-system-profile

14.1.165 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp restart-delay 1
```

Related Topics

14.1.98 display ap-system-profile

14.1.166 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** }

 Copyright © Huawei Technologies Co., Ltd.

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

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, TLVs defined by IEEE 802.1, and TLVs defined by IEEE 802.3 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.	-

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.

 Copyright © Huawei Technologies Co., Ltd.

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 802.1 format, TLVs in the IEEE 802.3 format.

Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.1 format, 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 IEEE 802.1 format, 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 is enabled globally and on interfaces.

Precautions

When the supported TLVs are basic TLVs, TLVs in the IEEE 802.1 format, and TLVs in the IEEE 802.3 format, the **lldp tlv-enable** command with the **all** parameter advertises all TLVs.

If the **all** parameter is not specified, only one type of TLV can be advertised. 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 ac
[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

14.1.15 ap lldp enable

14.1.160 lldp enable

14.1.167 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] log-server ip-address 10.0.0.1
```

14.1.168 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.

Copyright © Huawei Technologies Co., Ltd.

Table 14-84 Default lower temperature alarm threshold for APs

AP Model	Default Value (°C)
AP6010SN-GN/AP6010DN-AGN/ AP6310SN-GN/AP7110DN-AGN/ AP7110SN-GN/AP9330DN	-13
AP6510DN-AGN/AP6610DN-AGN/ AP6510DN-AGN-US/AP6610DN-AGN-US/AP8030DN/AP8130DN/AP9131DN	-43
AP5030DN/AP5130DN	-28
AP7030DE	-23

NOTE

The AP2010DN, AP2030DN, AP3010DN-AGN, AP5010SN-GN, AP5010DN-AGN, AP4030DN 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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] low-temperature threshold 5
```

Related Topics

14.1.98 display ap-system-profile

14.1.169 management-vlan

Function

The **management-vlan** command configures a management VLAN for an AP.

The **undo management-vlan** command deletes a management VLAN of an AP.

By default, no management VLAN is configured for an AP.

Format

management-vlan *vlan-id*

undo management-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the management VLAN.	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, the management packets of APs are untagged, and the access switch directly connected to the APs tag VLAN IDs on the management packets.

After the **management-vlan** command is executed, the management and control packets sent from APs to the AC contain the management VLAN tag. You can use this command according to the networking.

Precautions

The configured management VLAN takes effect only after the AP is restarted.

 Copyright © Huawei Technologies Co., Ltd.

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 AP's management VLAN is configured using the **management-vlan** *vlan-id* command, packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in untagged mode using the **vlan untagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command, the packets sent from the AP's wired interface are not tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in tagged mode using the **vlan tagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the PVID of the AP's wired interface is set to the management VLAN ID using the **vlan pvid** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.

Example

Set the management VLAN of the AP to VLAN 2 in the AP system profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] management-vlan 2
Warning: This operation will cause AP reset. Continue? [Y/N]:y
```

Related Topics

14.1.98 display ap-system-profile

14.5.15 vlan pvid (AP wired port profile view)

14.5.17 vlan (AP wired port profile view)

14.1.170 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

 Copyright © Huawei Technologies Co., Ltd.

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 128.

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 the number of successfully associated STAs on a VAP reaches the maximum, new users cannot connect to the VAP.

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

Example

Set the maximum number of successfully associated STAs on a VAP to 50.

```
<Huawei> system-view
[Huawei] wlan ac
[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
```

14.1.171 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.

 Copyright © Huawei Technologies Co., Ltd.

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 to 60.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] memory-usage threshold 60
```

Related Topics

14.1.98 display ap-system-profile

14.1.172 mtu

Function

The **mtu** command changes the maximum transmission unit (MTU) of Ethernet ports in an AP system profile.

 Copyright © Huawei Technologies Co., Ltd.

The **undo mtu** command restores the default MTU of Ethernet ports in an AP system profile.

The default the MTU of Ethernet ports in an AP system profile 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 an Ethernet port.	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 an Ethernet interface of the 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

Change the MTU of Ethernet ports to 1700 bytes in the AP system profile.

```
<Huawei> system-view
[Huawei] wlan ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] mtu 1700
```

Related Topics

14.1.98 display ap-system-profile

14.1.173 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 11 Mbps in a 2G radio profile and 6 Mbps in a 5G radio profile.

Format

multicast-rate *multicast-rate*

undo multicast-rate

Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 2.4G radio profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] multicast-rate 54
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.188 radio-type (2G radio profile view)

14.1.174 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 begin or end with double quotation marks (" ").
all	Deletes all AP wired port link profiles.	-

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.175 port-link-profile (AP wired port profile view)** command to bind it to an AP wired port profile and then run the **14.1.241 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 ac
[Huawei-wlan-view] port-link-profile name port-link1
[Huawei-wlan-port-link-prof-port-link1]
```

Related Topics

14.1.104 display port-link-profile

14.1.175 port-link-profile (AP wired port profile view)

14.1.175 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.174 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 ac
[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

14.1.109 display references port-link-profile

14.1.128 display wired-port-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.174 port-link-profile (WLAN view)

14.1.176 priority-map downstream dscp

Function

The **priority-map downstream dscp** command configures mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets when packets are sent to an AP from upper-layer devices.

The **undo priority-map downstream** command restores the default mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets when packets are sent to an AP from upper-layer devices.

Table 14-85 describes the default mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets.

Table 14-85 Default mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets

DSCP	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 downstream dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot11e** *dot11e-value*

undo priority-map downstream

 Copyright © Huawei Technologies Co., Ltd.

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 UP value.	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 802.11e packets use different fields to identify their priorities. 802.11e 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 AC or upper-layer network to an AP, the AP needs to convert the 802.3 packets to 802.11e packets and map the ToS field in the IP packet header to the UP field of 802.11e packets. You can use the **priority-map downstream dscp** command to configure mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets.

Example

Configure mapping from DSCP priorities to user priorities in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map downstream dscp 0 to 6 dot11e 1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.124 display traffic-profile

14.1.177 priority-map downstream trust

Function

The **priority-map downstream trust** command configures mapping from the 802.1p or DSCP priority of 802.3 packets to the 802.11e user priority of 802.11 packets when packets are forwarded to APs from upper-layer network devices.

The **undo priority-map downstream trust** command restores the default mapping from the 802.1p or DSCP priority of 802.3 packets to the 802.11e user priority of 802.11 packets when packets are forwarded to APs from upper-layer network devices.

By default, the 802.1p or DSCP priorities are mapped to 802.11e user priorities.

Format

priority-map downstream trust { **dot1p** | **dscp** }

undo priority-map downstream trust

Parameters

Parameter	Description	Value
dot1p	Specifies mapping from the 802.1p priority to the 802.11e user priority.	-
dscp	Specifies mapping from the DSCP priority to the 802.11e user 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

 Copyright © Huawei Technologies Co., Ltd.

802.3 packet header to the user priority of 802.11 packets. You can use the **priority-map downstream trust** command to configure mapping from the 802.1p or DSCP priority of 802.3 packets to the 802.11e user priority of 802.11 packets.

Example

Configure mapping from the 802.1p priority to the 802.11e user priority in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map downstream trust dot1p
```

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.124 display traffic-profile

14.1.178 priority-map tunnel-upstream dot11e

Function

The **priority-map tunnel-upstream dot11e** command configures mapping from the 802.11e user priority to DSCP priority in the CAPWAP header when packets are sent from an AP to an AC.

The **undo priority-map tunnel-upstream** command restores the default mapping from the 802.11e user priority to DSCP priority in the CAPWAP header when packets are sent from an AP to an AC.

By default, the 802.11e user priority is mapped to the DSCP priority in the CAPWAP header, as shown in **Table 14-86**.

NOTE

The CAPWAP header refers to the tunnel header.

Table 14-86 Default mapping from the 802.11e user priority to DSCP priority in the CAPWAP header

802.11e UP	DSCP Priority in the CAPWAP Header
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Copyright © Huawei Technologies Co., Ltd.

Format

priority-map tunnel-upstream dot11e { *dot11e-value1* [**to** *dot11e-value2*] } &<1-10> **dscp** *dscp-value*

undo priority-map tunnel-upstream

Parameters

Parameter	Description	Value
dot11e *dot11e-value1*	Specifies the 802.11e UP value.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
to *dot11e-value2*	Specifies the 802.11e UP value.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
dscp *dscp-value*	Specifies the DSCP priority in the CAPWAP header.	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

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.

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

Map 802.11e user priority 6 to DSCP priority 1 when packets are transmitted from an AP to an AC in the traffic profile **p1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map tunnel-upstream dot11e 6 dscp 1
```

Related Topics

14.1.124 display traffic-profile

14.1.229 traffic-profile (WLAN view)

14.1.179 priority-map tunnel-upstream dscp

Function

The **priority-map tunnel-upstream dscp** command configures mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to an AP.

The **undo priority-map tunnel-upstream dscp** command restores the default mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets.

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

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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	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

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.

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

Map DSCP priority 6 of 802.11 packets to DSCP priority 1 of tunnel packets when packets are sent to an AP in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map tunnel-upstream dscp 6 tunnel-dscp 1
```

Related Topics

14.1.124 display traffic-profile

14.1.229 traffic-profile (WLAN view)

14.1.180 priority-map tunnel-upstream trust

Function

The **priority-map tunnel-upstream trust** command configures mapping from the 802.11e user priority or DSCP priority of 802.3 packets to the user priority of tunnel packets.

The **undo priority-map tunnel-upstream trust** command restores the default mapping.

By default, the 802.11e user priority of 802.3 packets is mapped to the user priority of tunnel packets.

 Copyright © Huawei Technologies Co., Ltd.

Format

priority-map tunnel-upstream trust { **dot11e** | **dscp** }

undo priority-map tunnel-upstream trust

Parameters

Parameter	Description	Value
dot11e	Maps the 802.11e user priority of 802.3 packets to the user priority of tunnel packets.	-
dscp	Maps the DSCP priority of 802.3 packets to the user priority of tunnel packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

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.

Example

Configure mapping from the DSCP priority to the user priority of tunnel packets in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map tunnel-upstream trust dscp
```

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.124 display traffic-profile

14.1.181 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.

 Copyright © Huawei Technologies Co., Ltd.

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 and improve channel usage efficiency, 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 ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] probe-response-retry 0
```

Related Topics

14.1.118 display ssid-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.182 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 ac
[Huawei-wlan-view] ap-id 0
[Huawei-wlan-ap-0] radio 0
[Huawei-wlan-radio-0/0]
```

Related Topics

14.1.70 display ap

 Copyright © Huawei Technologies Co., Ltd.

14.1.183 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 cancels the status configuration of an AP radio. The status of the AP radio is then determined by the status 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.

After a radio is disabled, coverage hole compensation is triggered for automatic optimization.

Precautions

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

Example

Disable radio 0 of AP 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] radio disable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

14.1.184 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 begin 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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.185 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.

Usually, radio 0 and radio 1 of an AP work on the 2.4 GHz and 5 GHz frequency bands respectively. Only radio 0 of the AP2010DN and AP8130DN can be configured to work on the 2.4 GHz or 5 GHz frequency band using the **14.1.143 frequency** command.

Example

Create the 2G radio profile **radio-profile1** and display the view of the profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name radio-profile1
[Huawei-wlan-radio-2g-prof-radio-profile1]
```

Related Topics

14.1.106 display radio-2g-profile

14.1.186 radio-5g-profile (WLAN view)

14.1.185 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.184 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 ac
[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

14.1.97 display ap-group

14.1.110 display references radio-2g-profile

14.1.184 radio-2g-profile (WLAN view)

 Copyright © Huawei Technologies Co., Ltd.

14.1.186 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 begin 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

 Copyright © Huawei Technologies Co., Ltd.

Run the **14.1.187 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.

Usually, radio 0 and radio 1 of an AP work on the 2.4 GHz and 5 GHz frequency bands respectively. Only radio 0 of the AP2010DN and AP8130DN can be configured to work on the 2.4 GHz or 5 GHz frequency band using the **14.1.143 frequency** command.

Example

Create the 5G radio profile **radio-profile2** and display the view of the profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name radio-profile2
[Huawei-wlan-radio-5g-prof-radio-profile2]
```

Related Topics

14.1.107 display radio-5g-profile

14.1.184 radio-2g-profile (WLAN view)

14.1.187 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
radio *id*	Specifies the radio ID.	The value is an integer that ranges from 0 to 2.
radio all	Specifies all radios.	-

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a 5G radio profile using the **14.1.186 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 ac
[Huawei-wlan-view] radio-5g-profile name radio-profile2
[Huawei-wlan-radio-5g-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

14.1.97 display ap-group

14.1.111 display references radio-5g-profile

14.1.186 radio-5g-profile (WLAN view)

14.1.188 radio-type (2G radio profile view)

Function

The **radio-type** command sets the radio type in a 2G radio profile.

Copyright © Huawei Technologies Co., Ltd.

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 view

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 legacy terminals becomes invalid.

If WDS-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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the radio type to **dot11g** in a 2G radio profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] radio-type dot11g
```

Related Topics

14.1.44 beacon-2g-rate

14.1.106 display radio-2g-profile

14.1.173 multicast-rate

14.1.189 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** | **dot11ac** | **dot11n** }

undo radio-type

Parameters

Parameter	Description	Value
dot11a	Specifies the 802.11a radio type.	-
dot11ac	Specifies the 802.11a/n/ac radio type.	-
dot11n	Specifies the 802.11a/n radio type.	-

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

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 legacy terminals 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-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 ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] radio-type dot11n
```

Related Topics

14.1.107 display radio-5g-profile

14.1.190 rate-limit

Function

The **rate-limit** command configures 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 of upstream and downstream packets configured for all STAs on a VAP using the **rate-limit vap** command must be greater than or equal to that configured for each STA on a VAP using the **rate-limit client** command.

The limited rate of upstream and downstream packets configured for each STA on a VAP using the **rate-limit client** command cannot exceed that configured for all STAs on a VAP using the **rate-limit vap** command.

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 ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] rate-limit vap up 4294967295
```

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.124 display traffic-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.191 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 ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] reach-max-sta hide-ssid disable
```

Related Topics

14.1.118 display ssid-profile

Copyright © Huawei Technologies Co., Ltd.

14.1.192 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 begin 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.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Run the **14.1.193 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 ac
[Huawei-wlan-view] regulatory-domain-profile name domain1
[Huawei-wlan-regulate-domain-domain1]
```

Related Topics

14.1.117 display regulatory-domain-profile

14.1.193 regulatory-domain-profile

14.1.193 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.

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.

 Copyright © Huawei Technologies Co., Ltd.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a regulatory domain profile using the **14.1.192 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 ac
[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

14.1.97 display ap-group

14.1.112 display references regulatory-domain-profile

14.1.192 regulatory-domain-profile (WLAN view)

14.1.194 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ab
[Huawei-wlan-ap-system-prof-ab] report-disassoc-request disable
```

14.1.195 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

 Copyright © Huawei Technologies Co., Ltd.

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

14.1.80 display ap offline-record

14.1.196 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

 Copyright © Huawei Technologies Co., Ltd.

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

14.1.81 display ap online-fail-record

14.1.197 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear information about unauthenticated APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] reset ap unauthorized record
Warning: Clear unauthorized AP record, continue?[Y/N]:y
```

Related Topics

14.1.89 display ap unauthorized record

14.1.198 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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.101 display channel switch-record

14.1.199 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.	Currently, only Ethernet interfaces are supported.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

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

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

14.1.200 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

 Copyright © Huawei Technologies Co., Ltd.

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.

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

14.1.120 display station assoc-info ap-offline-record

14.1.201 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

 Copyright © Huawei Technologies Co., Ltd.

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

14.1.122 display station offline-record

14.1.202 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

 Copyright © Huawei Technologies Co., Ltd.

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

14.1.121 display station online-fail-record

14.1.203 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

Copyright © Huawei Technologies Co., Ltd.

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

14.1.123 display station statistics

14.1.204 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.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system view
[Huawei] wlan ac
[Huawei-wlan-view] reset statistics ap-name area1
```

14.1.205 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 four 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 ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[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 14-87 Description of the **rf-ping** command output

Item	Description
Tx rate	Transmission rate.
RSSI	Received signal strength.
time	Packet transmission delay.

14.1.206 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 **cts-to-self**.

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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] rts-cts-mode rts-cts
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.207 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 2347 bytes.

 Copyright © Huawei Technologies Co., Ltd.

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 an 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 ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] rts-cts-threshold 2300
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.208 service-vlan

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* }

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.

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. 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.

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 ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] service-vlan vlan-id 2
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.127 display vap-profile

14.1.209 set workmode wlan

Function

The **set workmode wlan** command configures the WLAN mode of the device.

By default, the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW work in AP mode and other devices work in AC mode.

Format

set workmode wlan { **ap** | **ac** }

Parameters

Parameter	Description	Value
ap	Indicates that the device works in Fat AP mode.	-
ac	Indicates that the device works in AC mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Fat AP mode, the device functions as an access point (AP) to provide access control, authentication, data encryption, and QoS functions.

In AC mode, the device functions as the access controller (AC) to deploy and control APs. The AC implements functions including mobility management, identity verification, VLAN assignment, radio resource management, wireless Intrusion Detection System (IDS), and data packet forwarding. APs only send and

 Copyright © Huawei Technologies Co., Ltd.

receive wireless data, simplifying AP management and configuration. APs can even work without any configuration.

Example

Configure the device to work in AC mode.

```
<Huawei> system-view
[Huawei] set workmode wlan ac
Warning: The WorkMode Change will be activated after board reboot. Continue? [y/n]:y
[Huawei] quit
<Huawei> reboot fast
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

14.1.210 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 ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] sftp server disable
```

Related Topics

14.1.98 display ap-system-profile

14.1.211 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, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

The preamble is a section of bits in the header of a data frame. It synchronizes signals transmitted between the sender and receiver. The preamble is classified into the long preamble and short preamble. The short preamble ensures better synchronization performance and therefore is recommended. The long preamble is usually used for compatibility with earlier network adapters of clients.

Example

Configure the 2G radio profile **default** not to support the short preamble.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] short-preamble disable
```

Related Topics

14.1.106 display radio-2g-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.107 display radio-5g-profile

14.1.212 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 ac
[Huawei-wlan-view] port-link-profile name port-link1
[Huawei-wlan-port-link-prof-port-link1] shutdown
Warning: The AP may become out of management after the port is disabled (if the port is an uplink port).
Continue?[Y/N]:y
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.104 display port-link-profile

14.1.213 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
```

 Copyright © Huawei Technologies Co., Ltd.

14.1.214 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 in text format and can contain 1 to 32 case-sensitive characters. It does not support Chinese 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

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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the SSID to **wlan-net** in the SSID profile **ssid1**.

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

Related Topics

14.1.118 display ssid-profile

14.1.215 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

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

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Configure SSID hiding in Beacon frames in the SSID profile **ssid1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] ssid-hide enable
```

Related Topics

14.1.118 display ssid-profile

14.1.216 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 begin or end with double quotation marks (" ").
all	Deletes all SSID profiles.	-

Copyright © Huawei Technologies Co., Ltd.

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, and legacy terminal access.

Follow-up Procedure

Run the **14.1.217 ssid-profile (VAP profile view)** command to bind the SSID profile to a VAP profile and run the **14.1.234 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.

  ```
  Warning: This action may cause service interruption. Continue?[Y/N]
  ```

Example

Create an SSID profile **ssid1** and enter the SSID profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1]
```

Related Topics

14.1.127 display vap-profile

14.1.217 ssid-profile (VAP profile view)

14.1.217 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.216 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 ac
[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

14.1.113 display references ssid-profile

14.1.127 display vap-profile

14.1.216 ssid-profile (WLAN view)

 Copyright © Huawei Technologies Co., Ltd.

14.1.218 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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] stelnet server disable
```

Related Topics

14.1.98 display ap-system-profile

14.1.219 telnet enable

Function

The **telnet enable** command enables Telnet on an AP.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] telnet enable
```

Related Topics

14.1.98 display ap-system-profile

14.1.218 stelnet server disable

14.1.220 temporary-management enable (AP system profile view)

Function

The **temporary-management enable** command enables offline management VAP and antenna alignment VAP functions.

 Copyright © Huawei Technologies Co., Ltd.

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 offline management VAP function is enabled for an AP, the AP automatically generates a management VAP when it becomes faulty. The default SSID and password of the management VAP are **hw_manage_xxxx** and **hw_manage** respectively. **xxxx** indicates the last four bits of the AP's MAC address. To troubleshoot the AP fault, the maintenance personnel only need to set the IP address of the maintenance device to 169.254.2.x/16 (except 169.254.2.1. This IP address is used only to facilitate fault location and needs to be changed when fault location is completed), associate the device to the wireless network with SSID **hw_manage_xxxx**, and connect to the AP using Telnet. This prevents complex operations.
- 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** and **hw_manage** respectively. **xxxx** indicates the last four bits of the AP's MAC address. You can associate the mobile phone on which the antenna alignment 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.

Precautions

- After the offline management VAP and antenna alignment VAP functions are enabled, the administrator needs to change the SSIDs and passwords of the

 Copyright © Huawei Technologies Co., Ltd.

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 antenna alignment 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 works only on the 2.4 GHz radio. If the 2.4 GHz radio is occupied by the WDS bridge, the offline management VAP function cannot be used.
- Before using the offline management VAP function, ensure that the AP has enabled with Telnet 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 then run 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, an RRU automatically generates an offline management VAP when it is disconnected from the central AP. Packets of the offline management VAP are only processed on the RRU and wil not be forwarded to the central AP. If the link between the central AP and AC is disconnected, all online RRUs on the central AP will automatically generate an offline management VAP, and send packets of the VAPs to the central AP for processing. The central AP does not have radios and therefore do not generate an offline management VAP.

Example

Enable offline management VAP and antenna alignment VAP functions.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name apsys1
[Huawei-wlan-ap-system-prof-apsys1] temporary-management enable
```

Related Topics

14.1.98 display ap-system-profile

14.1.221 temporary-management enable (VAP profile view)

 Copyright © Huawei Technologies Co., Ltd.

14.1.221 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** and **hw_manage** respectively. **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** and **hw_manage** respectively. **xxxx** indicates the last four bits of the AP's MAC address. Using the default antenna alignment VAP also brings security risks.

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

 Copyright © Huawei Technologies Co., Ltd.

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 works only on the 2.4 GHz radio. If the 2.4 GHz radio is occupied by the WDS bridge, the offline management VAP function cannot be used.
- 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.

Example

Configure VAPs generated by the VAP profile **vap1** as the offline management VAP and antenna alignment VAP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] temporary-management enable
```

Related Topics

14.1.98 display ap-system-profile

14.1.220 temporary-management enable (AP system profile view)

14.1.222 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.

 Copyright © Huawei Technologies Co., Ltd.

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 allowed on an AP's wired interface.	-
multicast-suppression	Specifies the maximum multicast traffic volume allowed on an AP's wired interface.	-
unicast-suppression	Specifies the maximum unknown unicast traffic volume allowed 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

 Copyright © Huawei Technologies Co., Ltd.

Bind the AP wired port profile to an AP group or AP.

Precautions

The uplink interfaces of RRUs do not support this command.

Example

Set the maximum broadcast traffic volume allowed on an AP's wired interface to 21600 pps.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wire1
[Huawei-wlan-wired-port-wire1] traffic-optimize broadcast-suppression packets 21600
```

Related Topics

14.1.128 display wired-port-profile

14.1.223 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize broadcast-suppression packets 21600
```

14.1.224 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize multicast-suppression packets 21600
```

14.1.225 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize multicast-unicast enable
```

14.1.226 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize sta-bridge-forward disable
```

14.1.227 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize unicast-suppression packets 21600
```

14.1.228 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.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The traffic profile has been created using the **14.1.229 traffic-profile (WLAN view)** command.

Example

Create VAP profile **p1** and bind traffic profile **u1** to the VAP profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name p1
[Huawei-wlan-vap-prof-p1] traffic-profile u1
```

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.124 display traffic-profile

14.1.229 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 begin or end with double quotation marks (" ").
all	Deletes all traffic profiles.	–

Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1]
```

Related Topics

14.1.124 display traffic-profile

14.1.230 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

 Copyright © Huawei Technologies Co., Ltd.

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 **service**, STAs connected to the VAP can only access network resources but not APs. Service VAPs are used in regular WLAN deployment scenarios.
- If the type of a VAP is set to **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.

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, configure an IP address in the same network segment as the AP for a STA, 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 ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] type ap-management
```

Related Topics

14.1.127 display vap-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.231 undo ap

Function

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

Format

undo ap { **ap-name** *ap-name* | **ap-id** *ap-list* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Deletes the AP with 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.
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

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Delete the AP named **Area_1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] undo ap ap-name Area_1
Warning: Deleting the AP will interrupt user services. Continue?[Y/N]:y
```

Related Topics

14.1.70 display ap

14.1.232 utmost-power disable

Function

The **utmost-power disable** command disables radios from sending packets at maximum power.

The **undo utmost-power disable** command enables radios to send packets at maximum power.

By default, a radio can send packets at 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

The command takes effect only for the country code CN. You can use the command to configure a radio to send packets at maximum power supported by

 Copyright © Huawei Technologies Co., Ltd.

the radio or maximum power allowed by the country code. After a radio is disabled from sending packets at maximum power, the radio uses the maximum power allowed by the country code to send packets.

Except the country code CN, a radio can only send packets using the maximum power allowed by the country codes.

Precautions

Only radios of the AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN can send packets at maximum power.

Example

Disable radios from sending packets at maximum power.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] utmost-power disable
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.233 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** }

 Copyright © Huawei Technologies Co., Ltd.

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 begin or end with double quotation marks (" ").
all	Deletes all VAP profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a radio profile is 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 **14.1.234 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a VAP profile **vap1** and enter the VAP profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1]
```

Related Topics

14.1.127 display vap-profile

14.1.234 vap-profile

14.1.234 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** } }

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.
radio	Specifies a radio.	-
radio-id	Specifies a radio ID.	The value is an integer that ranges from 0 to 2.
all	Specifies all radios.	-

Views

AP group view, AP view, AP radio view, AP group radio view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VAP profile using the **14.1.233 vap-profile (WLAN view)** command, bind it to a radio so that the VAP profile can take effect.

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 ac
[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

14.1.97 display ap-group

14.1.115 display references vap-profile

14.1.233 vap-profile (WLAN view)

14.1.235 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 AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN support 802.11ac.

Format

vht a-mpdu max-length-exponent *max-length-exponent-index*

undo vht a-mpdu max-length-exponent

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] vht a-mpdu max-length-exponent 2
```

Related Topics

14.1.107 display radio-5g-profile

14.1.236 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 AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN support 802.11ac.

Format

vht a-msdu enable

undo vht a-msdu enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] vht a-msdu enable
```

Related Topics

14.1.107 display radio-5g-profile

14.1.237 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 AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN support 802.11ac.

Format

vht a-msdu max-frame-num *max-frame-number*

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.236 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 ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] vht a-msdu max-frame-num 3
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.236 vht a-msdu enable

14.1.107 display radio-5g-profile

14.1.238 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 AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN 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

 Copyright © Huawei Technologies Co., Ltd.

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.

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 ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] vht mcs-map nss 2 max-mcs 8
```

Related Topics

14.1.107 display radio-5g-profile

14.1.239 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 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 functions are disabled on an AP, the blinking frequency of the Wireless LED reflects the service traffic volume on the radio.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only APs having Wireless LEDs support this command.

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.	-
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 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 function enabled. If the WDS functions are disabled on the AP, the Wireless LED always shows service traffic volume.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-2g-profile name radio-profile1
[Huawei-wlan-radio-2g-prof-radio-profile1] wifi-light traffic
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.240 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 begin or end with double quotation marks (" ").
all	Deletes all AP wired port profiles.	-

Views

WLAN view

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.241 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 ac
[Huawei-wlan-view] wired-port-profile name wired-port1
[Huawei-wlan-wired-port-wired-port1]
```

Related Topics

14.1.128 display wired-port-profile

14.1.241 wired-port-profile (AP group view and view)

14.1.241 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*

 Copyright © Huawei Technologies Co., Ltd.

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 **14.1.240 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 ac
[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

14.1.97 display ap-group

14.1.116 display references wired-port-profile

14.1.240 wired-port-profile (WLAN view)

 Copyright © Huawei Technologies Co., Ltd.

14.1.242 wlan

Function

The **wlan ac** command displays the WLAN view.

Format

wlan ac

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 ac
[Huawei-wlan-view]
```

14.1.243 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

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

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 ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] undo wmm disable
```

Related Topics

14.1.184 radio-2g-profile (WLAN view)
14.1.186 radio-5g-profile (WLAN view)

14.1.244 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 14-88 lists the default EDCA parameter settings and ACK policies for APs.

Table 14-88 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

Copyright © Huawei Technologies Co., Ltd.

Format

wmm edca-ap { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } } *

undo wmm edca-ap

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the AIFSN, which determines the channel idle time.	The value is an integer that ranges from 1 to 15.
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 cannot be greater than 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 cannot be smaller than 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 microseconds. **NOTE** If the *txoplimit-value* value is 0, the STA can send only one data frame every time it occupies a channel.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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. The **noack** is applicable to scenarios with good communication quality and little interference.	-

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.

Example

Set EDCA parameters and ACK policies for AC_VO packets in 5G radio profile **default**.

```
<Huawei> system-view
[Huawei] wlan ac
[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
```

 Copyright © Huawei Technologies Co., Ltd.

14.1.245 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 14-89 lists the default EDCA parameter settings for STAs.

Table 14-89 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 the *ecwmax-value* value.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ecwmax *ecwmax-value*	Specifies the exponent form of the maximum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than the *ecwmin-value* value.
txoplimit *txoplimit-value*	Specifies the transmission opportunity limit (TXOPLimit), which determines the maximum duration in which an 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 14-90 describes the EDCA parameters.

Table 14-90 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Meaning
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 **14.1.243 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.

Example

Set EDCA parameters for AC_VO packets of STAs in SSID profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.1.118 display ssid-profile

14.1.246 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

Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] wmm mandatory enable
```

14.2 WLAN Radio Resource Management Configuration Commands

14.2.1 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**.

Format

amc-policy { **auto-balance** | **high-stability** | **high-throughput** }

undo amc-policy

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] amc-policy high-stability
```

Related Topics

14.2.20 display rrm-profile

14.2.2 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.

 Copyright © Huawei Technologies Co., Ltd.

By default, the system provides the air scan profile **default**. You can run the **14.2.17 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 begin 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, 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, or WIDS data analysis.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

Run the **14.2.3 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 ac
[Huawei-wlan-view] air-scan-profile name air-scan01
[Huawei-wlan-air-scan-prof-air-scan01]
```

Related Topics

14.2.3 air-scan-profile (radio profile view)

14.2.3 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 **14.2.2 air-scan-profile** command, bind it to a radio profile so that the air scan profile can take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind the air scan profile **air-scan01** to the radio profile **office01**.

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.2.2 air-scan-profile

14.2.4 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	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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.2.5 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 x 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 preceding formula 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 ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] band-steer balance gap-threshold 25
```

Related Topics

14.2.7 band-steer deny-threshold

14.2.5 band-steer balance start-threshold

14.2.5 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 10.

Format

band-steer balance start-threshold *start-threshold*

undo band-steer balance start-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
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 **14.2.4 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 ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] band-steer balance start-threshold 20
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.2.4 band-steer balance gap-threshold

14.2.7 band-steer deny-threshold

14.2.6 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] band-steer client-band-expire 80
```

14.2.7 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 2.

Format

band-steer deny-threshold *deny-threshold*

undo band-steer deny-threshold

 Copyright © Huawei Technologies Co., Ltd.

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 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 ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] band-steer deny-threshold 8
```

Related Topics

14.2.8 band-steer disable

14.2.8 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] vap-profile name huawei
[Huawei-wlan-vap-prof-huawei] band-steer disable
```

Related Topics

14.1.127 display vap-profile

 Copyright © Huawei Technologies Co., Ltd.

14.2.9 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 in the AP's RRM profile.

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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable automatic channel selection in the RRM profile **802.11b**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name 802.11b
[Huawei-wlan-rrm-prof-802.11b] calibrate auto-channel-select disable
```

14.2.10 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 in the AP's RRM profile.

Example

Disable automatic transmit power selection in the RRM profile **802.11b**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name 802.11b
[Huawei-wlan-rrm-prof-802.11b] calibrate auto-txpower-select disable
```

14.2.11 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 00:00:00.

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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
schedule	Sets the radio calibration mode to schedule.	-
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:

- Auto mode: The device periodically implements radio calibration at certain intervals (the interval is specified by **interval** and the default interval is 1440 minutes).
- Manual mode: Radio calibration is not automatically implemented by the device but manually triggered through the **14.2.13 calibrate manual startup** command.
- Schedule 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 ac
[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.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] calibrate enable schedule time 20:30:00
```

Related Topics

14.2.13 calibrate manual startup

14.2.12 calibrate error-rate-threshold

Function

The **calibrate error-rate-threshold** command sets the packet error rate (PER) threshold in a radio profile.

The **undo calibrate error-rate-threshold** command restores the default PER threshold in a radio profile.

By default, the PER 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 PER threshold.	The value is an integer that ranges from 20 to 80, 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 PER threshold determines whether the radio environment is normal. When the PER 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the PER threshold to 70% in the RRM profile **80211b**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name 80211b
[Huawei-wlan-rrm-prof-80211b] calibrate error-rate-threshold 70
```

14.2.13 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

When you need to implement radio calibration instantly, 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 ac
[Huawei-wlan-view] calibrate enable auto
[Huawei-wlan-view] calibrate manual startup
```

Related Topics

14.2.11 calibrate enable { auto | manual | schedule time }

14.2.14 calibrate sensitivity

 Copyright © Huawei Technologies Co., Ltd.

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: The device implements radio calibration when the current spectrum model is not as good as the estimated spectrum model.
- medium: The device implements radio calibration when the current spectrum model varies from the estimated spectrum model.
- low: The device implements radio calibration when the current spectrum model differs greatly from the estimated spectrum model.

The default value is recommended.

Example

Set the radio calibration sensitivity to high.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] calibrate sensitivity high
```

 Copyright © Huawei Technologies Co., Ltd.

14.2.15 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 **14.2.16 dca-channel channel-set** command to configure calibration channels as prompted.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

When the calibration bandwidth is changed, the device recalculates the calibration channels.

Precautions

Only the AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP9131DN, AP9330DN, AP8030DN, 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 ac
[Huawei-wlan-view] regulatory-domain-profile name huawei
[Huawei-wlan-regulate-domain-huawei] dca-channel 5g bandwidth 40mhz
```

Related Topics

14.2.16 dca-channel channel-set

14.1.117 display regulatory-domain-profile

14.2.16 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**

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

the 40 MHz and 80 MHz channels are fixed. For details, see *Huawei AR Series Access Routers Configuration Guide*–Radio Resource Management–Radio Calibration.

You can also use the **14.2.15 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. For example, when the country code is set to China, 5 GHz channels 36, 40, 44, 48, 52, 56, 60, and 64 can be configured. However, most terminals do not support these channels currently. If these channels are configured, the terminals cannot discover wireless signals. In this case, you can configure 5 GHz channels 149, 153, 157, 161, and 165, which are supported by the terminals.

Example

Configure a calibration channel set composed of 40MHz channels 149, 153, 157, and 161 on the 5 GHz frequency band.

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.1.61 country-code

14.2.15 dca-channel bandwidth

14.2.17 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 14-91 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 period(ms)   : 80
Scan interval(ms) : 3000
Scan channel-set  : dca-channel
------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-92 Description of the **display air-scan-profile name** command output

Item	Description
Scan period(ms)	Air scan period. To set the air scan period, run the **14.2.39 scan-period** command.
Scan interval(ms)	Air scan interval. To set the air scan interval, run the **14.2.38 scan-interval** command.
Scan channel-set	Air scan channel set. To set the air scan channel set, run the **14.2.37 scan-channel-set** command.

Related Topics

14.2.39 scan-period
14.2.38 scan-interval
14.2.37 scan-channel-set

14.2.18 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

 Copyright © Huawei Technologies Co., Ltd.

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 14-93 Description of the **display references air-scan-profile** command output

Item	Description
Reference type	Type of the profile that references the air scan profile.
Reference name	Name of the profile that references the air scan profile.

14.2.19 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

 Copyright © Huawei Technologies Co., Ltd.

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 14-94 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.

14.2.20 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 already exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rrm-profile** 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 14-95 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
Airtime fairness schedule                          : disable
Dynamic adjust EDCA parameter                      : enable
Band steer deny threshold                          : 2
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 start threshold               : 10
Station load balance gap threshold(%)              : 20
------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-96 Description of the **display rrm-profile name** command output

Item	Description
Auto channel select	Whether to enable automatic channel selection. To enable automatic channel selection, run the **14.2.9 calibrate auto-channel-select disable** command.
Auto transmit power select	Whether to enable automatic transmit power selection. To enable automatic transmit power selection, run the **14.2.10 calibrate auto-txpower-select disable** command.
PER threshold for trigger channel/ power select(%)	PER threshold for triggering channel or power adjustment. To set the PER threshold, run the **14.2.12 calibrate error-rate-threshold** command.
Airtime fairness schedule	Whether to enable airtime fair scheduling.
Dynamic adjust EDCA parameter	Whether to enable dynamic EDCA parameter adjustment. To enable dynamic EDCA parameter adjustment, run the **14.2.26 dynamic-edca enable** command.
Band steer deny threshold	Maximum number of times that an AP rejects association requests of a STA for band steering. To configure the maximum number of rejections, run the **14.2.7 band-steer deny-threshold** command.
Band balance start threshold	Start threshold for load balancing between radios. To configure start threshold for load balancing between radios, run the **14.2.5 band-steer balance start-threshold** command.
Band balance gap threshold(%)	Load difference threshold for load balancing between radios. To configure load difference threshold for load balancing between radios, run the **14.2.4 band-steer balance gap-threshold** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Client's band expire based on continuous probe counts	Aging condition of terminal band information, that is, the number of times that an AP has continuously received Probe frames of a terminal from the same frequency band. To set the aging condition of terminal band information, run the **14.2.6 band-steer client-band-expire** command.
Station load balance	Whether to enable the load balancing function. To configure the load balancing function, run the **14.2.40 sta-load-balance dynamic enable** command.
Station load balance start threshold	Start threshold for load balancing. To configure the start threshold for load balancing, run the **14.2.42 sta-load-balance dynamic start-threshold** command.
Station load balance gap threshold(%)	Load difference threshold for load balancing. To configure the load difference threshold for load balancing, run the **14.2.41 sta-load-balance dynamic gap-threshold** command.

Related Topics

14.2.9 calibrate auto-channel-select disable
14.2.10 calibrate auto-txpower-select disable
14.2.26 dynamic-edca enable
14.2.40 sta-load-balance dynamic enable
14.2.42 sta-load-balance dynamic start-threshold
14.2.41 sta-load-balance dynamic gap-threshold

14.2.21 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* }

Copyright © Huawei Technologies Co., Ltd.

Parameters

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

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display sta-load-balance static-group** command to view information about a specified static load balancing group or all static load balancing groups.

Example

Display information about all static load balancing group.

```
<Huawei> display sta-load-balance static-group all
-------------------------------------------------------------
Index  Group name
-------------------------------------------------------------
0      cc
1      coco
-------------------------------------------------------------
Total: 2
```

Table 14-97 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
Start threshold      : 5
```

 Copyright © Huawei Technologies Co., Ltd.

```
Gap threshold(%)     : 40
-------------------------------------------------------------
RfID: Radio ID
CurEIRP: Current EIRP (dBm)
Act CH: Actual channel, Cfg CH: Config channel
-------------------------------------------------------------
AP ID  AP Name  RfID  Act CH/Cfg CH  CurEIRP/MaxEIRP  Client
-------------------------------------------------------------
2      area_2   0     6/-            28/28            0
2      area_2   1     153/-          29/29            0
3      area_3   0     1/-            28/28            0
3      area_3   1     149/-          29/29            0
-------------------------------------------------------------
Total: 4
```

Table 14-98 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.
Start threshold	Start threshold for load balancing in a static load balancing group. To configure the parameter, run the **14.2.44 start-threshold** command.
Gap threshold(%)	Load difference threshold in a static load balancing group. To configure the parameter, run the **14.2.27 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.

Related Topics

14.2.44 start-threshold

14.2.27 gap-threshold

Copyright © Huawei Technologies Co., Ltd.

14.2.22 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
--------------------------------------------------------------------------------
ap1                             0
ap3                             0
--------------------------------------------------------------------------------
Total: 2
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-99 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.

14.2.23 display station rssi-rejected statistics

Function

The **display station rssi-rejected statistics** command displays information about rejected STAs by a specified VAP due to weak signal strength.

Format

display station rssi-rejected statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* **vap-profile** *profile-name*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must already exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must already exist.
radio *radio-id*	Specifies the radio ID.	The value is an integer that ranges from 0 to 2.
vap-profile *profile-name*	Specifies the ID of a service set.	The VAP profile must already exist.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The **display station rssi-rejected statistics** command displays information about rejected STAs due to weak signal strength.

Example

Display the number of times a STA is rejected due to weak signal strength in the VAP profile **office** applied to radio 0 of AP **huawei**.

```
<Huawei> display station rssi-rejected statistics ap-name huawei radio 0 vap-profile office
 Total station numbers: 2
--------------------------------------------------------------------------------
 MAC              Times    Last reject time
 c46a-b72c-4100   2        2012-07-23/09:26:23
 38e7-d87c-48c1   478      2012-07-23/10:16:10
--------------------------------------------------------------------------------
```

Table 14-100 Description of the **display station rssi-rejected statistics** command output

Item	Description
Total station numbers	Total number of STAs that are rejected due to weak signal strength.
MAC	MAC address of the rejected STA.
Times	Total number of times the STA is rejected.
Last reject time	Time when the STA is rejected for the last time.

14.2.24 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** }

 Copyright © Huawei Technologies Co., Ltd.

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 14-101 Description of the **display wlan calibrate channel-set** command output

Item	Description
AP group	Name of an AP group.
Country code	Country code.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Radio band	Radio type.
Bandwidth	Effective calibration bandwidth.
Channel Set	Effective calibration channel set.

Related Topics

14.2.15 dca-channel bandwidth
14.2.16 dca-channel channel-set

14.2.25 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.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

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 14-102 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

14.2.34 reset wlan calibrate statistics

14.2.26 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] dynamic-edca enable
```

Related Topics

14.2.20 display rrm-profile

14.2.27 gap-threshold

Function

The **gap-threshold** command sets the load difference threshold for a static load balancing group.

The **undo gap-threshold** command restores the default load difference threshold for a static load balancing group.

By default, the load difference threshold of a static load balancing group is 20%.

Format

gap-threshold *gap-threshold-value*

undo gap-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
gap-threshold-value	Specifies the load difference threshold.	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 number of STAs on radios.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

After the load difference threshold is configured using the **gap-threshold** command, the AP implements load balancing based on the difference between the number of users on different radios. The load balancing algorithm is as follows:

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 STAs on the radio/Maximum number of STAs 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 STA 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 (configured using the *gap-threshold-value* command). If the load difference is smaller than the threshold, the AC allows the STA to associate with the radio. If not, the AC rejects the association request of the STA. If the STA continues sending association requests to this AP, the AC allows the STA to associate with the AP when the number of consecutive association attempts of the STA exceeds the maximum value configured.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the load difference threshold to 40% for the static load balancing group **coco**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-load-balance static-group name coco
[Huawei-wlan-sta-lb-static-coco] gap-threshold 40
```

Related Topics

14.2.43 sta-load-balance static-group

14.2.28 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.

 Copyright © Huawei Technologies Co., Ltd.

After the **14.2.30 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 an alarm is generated.

Example

Set the alarm threshold for adjacent-channel interference to 52%.

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.2.30 interference detect-enable

14.2.29 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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.2.30 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 ac
[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

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile
14.2.30 interference detect-enable

14.2.30 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] radio-2g-profile name radio0
[Huawei-wlan-radio-2g-prof-radio0] interference detect-enable
```

14.2.31 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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.2.30 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 ac
[Huawei-wlan-view] radio-2g-profile name radio0
[Huawei-wlan-radio-2g-prof-radio0] interference station threshold 50
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.2.30 interference detect-enable

14.2.32 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

member { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] } &<1-16>

undo member { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] } &<1-16>

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of an AP. The AP name and radio ID identify a radio.	The AP name must exist.
ap-id *ap-id*	Specifies the ID of an AP. The AP ID and radio ID identify a radio.	The AP ID must exist.
radio *radio-id*	Specifies a radio ID. The radio ID and AP name identify a radio.	The value is an integer that ranges from 0 to 2.

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.

Example

Add radio 0 of AP **office** to the static load balancing group **coco**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-load-balance static-group name coco
[Huawei-wlan-sta-lb-static-coco] member ap-name office radio 0
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.2.43 sta-load-balance static-group

14.2.33 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable signal-strength-based power adjustment for APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name huawei
[Huawei-wlan-radio-2g-prof-huawei] power auto-adjust enable
```

Related Topics

14.2.10 calibrate auto-txpower-select disable

14.2.34 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.

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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear calibration statistics about radio 0 of AP **office**.

```
<Huawei> reset wlan calibrate statistics ap-name office radio 0
```

Related Topics

14.2.25 display wlan calibrate statistics

14.2.35 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**. You can run the **14.2.20 display rrm-profile** command to view configuration of 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 begin 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

Copyright © Huawei Technologies Co., Ltd.

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 **14.2.36 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 ac
[Huawei-wlan-view] rrm-profile name rrm01
[Huawei-wlan-rrm-prof-rrm01]
```

Related Topics

14.2.36 rrm-profile (radio profile view)

14.2.36 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.

 Copyright © Huawei Technologies Co., Ltd.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After you create an RRM profile using the **14.2.35 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 ac
[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

14.2.35 rrm-profile (WLAN view)

14.2.37 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dca-channel	Specifies a calibration channel set as the air scan channel set. To configure a calibration channel set, run the **14.2.16 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, 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. If the radio working mode is set to **monitor**, the AP scans all channels supported by the country code.

Example

Configure an air scan channel set that contains all calibration channels.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] air-scan-profile name huawei
[Huawei-wlan-air-scan-prof-huawei] scan-channel-set dca-channel
```

Related Topics

14.2.17 display air-scan-profile

 Copyright © Huawei Technologies Co., Ltd.

14.2.38 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 60000 ms.

Format

scan-interval *scan-time*

undo scan-interval

Parameters

Parameter	Description	Value
scan-time	Specifies an air scan interval.	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.

Precautions

The air scan interval also applies to radio calibration, 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.

Example

Set the air scan interval to 3000 ms for APs.

```
<Huawei> system-view
[Huawei] wlan ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] air-scan-profile name huawei
[Huawei-wlan-air-scan-prof-huawei] scan-interval 3000
```

Related Topics

14.2.17 display air-scan-profile

14.2.39 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, 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the air scan period to 80 ms for APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] air-scan-profile name huawei
[Huawei-wlan-air-scan-prof-huawei] scan-period 80
```

Related Topics

14.2.17 display air-scan-profile

14.2.40 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 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable dynamic load balancing.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] sta-load-balance dynamic enable
```

14.2.41 sta-load-balance dynamic gap-threshold

Function

The **sta-load-balance dynamic gap-threshold** command sets the load difference threshold for dynamic load balancing.

The **undo sta-load-balance dynamic gap-threshold** command restores the default load difference threshold for dynamic load balancing.

By default, the dynamic load difference threshold for load balancing is 20%.

Format

sta-load-balance dynamic gap-threshold *gap-threshold*

undo sta-load-balance dynamic gap-threshold

Parameters

Parameter	Description	Value
gap-threshold	Specifies the load difference threshold for dynamic load balancing.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

In dynamic load balancing mode, an AC uses a load balancing algorithm to determine whether to allow a STA to associate with a radio. The load balancing algorithm is as follows:

When a STA 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 **start-threshold** configured using the **14.2.42 sta-load-balance dynamic start-threshold** command, the AP does not implement dynamic load balancing. The AP

 Copyright © Huawei Technologies Co., Ltd.

implements dynamic load balancing only when the total number of access users on all radios exceeds **start-threshold**.

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 STAs on the radio/Maximum number of STAs 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 STA 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 load difference is smaller than the threshold, the AC allows the STA to associate with the radio. If not, the AC rejects the association request of the STA.

Example

Set the load difference threshold to 25 in the RRM profile **huawei**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] sta-load-balance dynamic gap-threshold 25
```

Related Topics

14.2.42 sta-load-balance dynamic start-threshold

14.2.42 sta-load-balance dynamic start-threshold

Function

The **sta-load-balance dynamic start-threshold** command sets the start threshold for dynamic load balancing.

The **undo sta-load-balance dynamic start-threshold** command restores the default start threshold for dynamic load balancing.

By default, the start threshold for dynamic load balancing is 10.

Format

sta-load-balance dynamic start-threshold *start-threshold*

undo sta-load-balance dynamic start-threshold

Parameters

Parameter	Description	Value
start-threshold	Specifies the start threshold for dynamic load balancing.	The value is an integer that ranges from 1 to 40.

 Copyright © Huawei Technologies Co., Ltd.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When a STA requests to connect to an AP, the AP will count the total number of access users on all radios. If the number of access users on the requested radio does not exceed **start-threshold**, the AP does not implement dynamic load balancing. The AP implements dynamic load balancing only after the number of access users exceeds **start-threshold**.

Example

Set the start threshold to 20 in the RRM profile **huawei**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] sta-load-balance dynamic start-threshold 20
```

Related Topics

14.2.41 sta-load-balance dynamic gap-threshold

14.2.43 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** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a load balancing group.	The value is a string of 1 to 35 plain-text characters. It does not contain any question mark (?) or spaces, 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 **14.2.32 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 ac
[Huawei-wlan-view] sta-load-balance static-group name new
[Huawei-wlan-sta-lb-static-new]
```

Related Topics

14.2.21 display sta-load-balance static-group

14.2.44 start-threshold

Function

The **start-threshold** command sets the start threshold for load balancing in a static load balancing group.

 Copyright © Huawei Technologies Co., Ltd.

The **undo start-threshold** command deletes the configured start threshold for load balancing in a static load balancing group.

By default, the start threshold for load balancing in a static load balancing group is 10.

Format

start-threshold *start-threshold-value*

undo start-threshold

Parameters

Parameter	Description	Value
start-threshold-value	Specifies the start threshold for load balancing 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 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 to 5 for the static load balancing group **coco**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-load-balance static-group name coco
[Huawei-wlan-sta-lb-static-coco] start-threshold 5
```

Related Topics

14.2.43 sta-load-balance static-group

14.3 WLAN Roaming Commands

 Copyright © Huawei Technologies Co., Ltd.

14.3.1 display station roam-track

Function

The **display station roam-track** command displays the roaming track of an 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 an 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)  Z:Zero Roam
--------------------------------------------------------------------------------
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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-103 Description of the **display station roam-track** command output

Item	Description
Access SSID	SSID associated with an STA.
Rx/Tx	Negotiated rate between the STA and AP.
Z	Zero Roam
L2/L3	Roaming mode.
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.
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 STA when it disconnects from an AP before roaming and goes online on an AP after roaming.
Out Rx/Tx	Negotiated rate of the STA when it disconnects from an AP.
Number	Number of STA roaming tracks.

14.4 WLAN Security Configuration Commands

14.4.1 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*

 Copyright © Huawei Technologies Co., Ltd.

undo brute-force-detect interval

Parameters

Parameter	Description	Value
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 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 **14.4.23 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 ac
[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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.4.55 wids attack detect enable
14.4.3 brute-force-detect threshold
14.4.23 dynamic-blacklist enable

14.4.2 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 a attack source launches attacks repeatedly, a large number of repetitive 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **14.4.23 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 ac
[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

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.3 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

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
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 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 **14.4.23 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 ac
[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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.4 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval at which an AP reports incremental wireless device information to 120 seconds.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wids-profile name office
[Huawei-wlan-wids-prof-office] device report-interval 120
```

14.4.5 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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.

Example

Set the interval at which an AP reports all wireless device information to 120 minutes.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wids-profile name office
[Huawei-wlan-wids-prof-office] device synchronization-interval 120
```

14.4.6 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
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
Reference type              Reference name
------------------------------------------------------------------------------
AP group                    default
AP ID                       0
------------------------------------------------------------------------------
Total: 2
```

Table 14-104 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.

14.4.7 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.

 Copyright © Huawei Technologies Co., Ltd.

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 14-105 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.

14.4.8 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

 Copyright © Huawei Technologies Co., Ltd.

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 14-106 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
Device synchronization interval(m)  : 120
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
WIDS spoof profile                  : huawei
-------------------------------------------------------------
```

Table 14-107 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 **14.4.4 device report-interval** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Device synchronization interval(m)	Interval at which an AP reports all the detected wireless device information. To set the interval, run the **14.4.5 device synchronization-interval** command.
Brute force detect interval(s)	Interval for brute force key cracking detection. To set the interval, run the **14.4.1 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 **14.4.3 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 **14.4.2 brute-force-detect quiet-time** command.
Flood detect interval(s)	Flood attack detection interval. To set the interval, run the **14.4.24 flood-detect interval** command.
Flood detect threshold	Flood attack detection threshold. To set the threshold, run the **14.4.26 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 **14.4.25 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 **14.4.52 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 **14.4.37 spoof-detect quiet-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dynamic blacklist	Whether the dynamic blacklist function is enabled. To configure the function, run the **14.4.23 dynamic-blacklist enable** command.
WIDS spoof profile	WIDS spoof profile bound to the WIDS profile. To bind a WIDS spoof profile to a WIDS profile, run the **14.4.59 wids-spoof-profile (WIDS profile view)** command.

Related Topics

14.4.4 device report-interval
14.4.5 device synchronization-interval
14.4.1 brute-force-detect interval
14.4.3 brute-force-detect threshold
14.4.2 brute-force-detect quiet-time
14.4.24 flood-detect interval
14.4.26 flood-detect threshold
14.4.25 flood-detect quiet-time
14.4.52 weak-iv-detect quiet-time
14.4.37 spoof-detect quiet-time
14.4.23 dynamic-blacklist enable
14.4.59 wids-spoof-profile (WIDS profile view)

14.4.9 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* }

Copyright © Huawei Technologies Co., Ltd.

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 14-108 Description of the **display wids-spoof-profile all** command output

Item	Description
Profile name	Name of a WIDS spoof SSID profile.
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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-109 Description of the **display wids-spoof-profile name** command output

Item	Description
ID	Index.
Pattern rule	Matching rule for spoofing SSIDs.

14.4.10 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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-110 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.

14.4.11 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
-----------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
VAP profile          vap-profile1
-----------------------------------------------
Total: 1
```

Table 14-111 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.

14.4.12 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**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display references sta-whitelist-profile name sta-whitelist-profile1
--------------------------------------------------------------------------------
Reference type              Reference name
--------------------------------------------------------------------------------
AP system profile           ap-system-profile1
--------------------------------------------------------------------------------
Total: 1
```

Table 14-112 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.

14.4.13 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display configurations of all security profiles.

```
<Huawei> display security-profile all
-------------------------------------------------------------
Profile name                Reference
-------------------------------------------------------------
default                     1
default-wds                 1

security-profile1           0
-------------------------------------------------------------
Total: 3
```

Table 14-113 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
-------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-114 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 **14.4.34 security wep**, **14.4.31 security dot1x**, **14.4.32 security psk** and **14.4.33 security wapi** commands.
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 **14.4.54 wep key**, **14.4.31 security dot1x** and **14.4.32 security psk** commands.
Key *key-id*	Key ID. To configure the parameter, run the **14.4.54 wep key** command.
Default key ID	Default key ID. To configure the parameter, run the **14.4.53 wep default-key** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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 **14.4.60 wpa ptk-update enable** command.
PTK update interval(s)	The interval for updating PTKs in WPA, WPA2 or WPA-WPA2 authentication and encryption. The value is an integer in seconds. To configure the parameter, run the **14.4.61 wpa ptk-update ptk-update-interval** command.
CA certificate filename	CA certificate file name. To configure the parameter, run the **14.4.45 wapi import certificate** command.
ASU certificate filename	File name of the authentication server unit (ASU) certificate. To configure the parameter, run the **14.4.45 wapi import certificate** command.
AC certificate filename	AC certificate file name. To configure the parameter, run the **14.4.45 wapi import certificate** command.
AC private key filename	AC private key file name. To configure the parameter, run the **14.4.46 wapi import private-key** command.
WAPI source interface	WAPI source interface. To configure the parameter, run the **14.4.50 wapi source interface** command.
Authentication server IP	IP address of the ASU certificate server. To configure the parameter, run the **14.4.42 wapi asu** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
WAI timeout(s)	Timeout period of an association. To configure the parameter, run the **14.4.49 wapi sa-timeout** command.
BK update interval(s)	Interval for updating the base key (BK). To configure the parameter, run the **14.4.43 wapi bk** command.
BK lifetime threshold(%)	Threshold for triggering BK update. To configure the parameter, run the **14.4.43 wapi bk** command.
USK update method	Whether the USK is updated based on a time interval or a packet count. To configure the parameter, run the **14.4.47 wapi key-update** command.
USK update interval(s)	Time-based interval for updating the unicast session key (USK). To configure the parameter, run the **14.4.51 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 **14.4.47 wapi key-update** command.
MSK update interval(s)	Time-based interval for updating the MBMS service key (MSK). To configure the parameter, run the **14.4.48 wapi msk** command.
Cert auth retrans count	Number of retransmissions of certificate authentication packets. To configure the parameter, run the **14.4.44 wapi cert-retrans-count** command.
USK negotiate retrans count	Number of retransmissions of USK negotiation packets. To configure the parameter, run the **14.4.51 wapi usk** command.
MSK negotiate retrans count	Number of retransmissions of MSK negotiation packets. To configure the parameter, run the **14.4.48 wapi msk** command.

 Copyright © Huawei Technologies Co., Ltd.

14.4.14 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 14-115 Description of the **display sta-blacklist-profile all** command output

Item	Description
Profile name	Name of a STA blacklist profile.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reference	Number of times a STA blacklist profile is referenced.

Display information about the STA blacklist profile **sta-blacklist-profile1**.

```
<Huawei> display sta-blacklist-profile name sta-blacklist-profile1
-------------------------------------------------------------
Index      MAC
-------------------------------------------------------------
0          0021-1111-2222
-------------------------------------------------------------
Total: 1
```

Table 14-116 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 **14.4.40 sta-mac** command.

Related Topics

14.4.40 sta-mac

14.4.15 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ap-name *ap-name*	Displays information about STAs that are denied access on the AP with a specified name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

There is a STA dynamic blacklist on an AP. The blacklist helps control access of STAs, for example, forbidding STAs with bogus IP addresses to go online. If a STA is not allowed to go online, the STA is added to the dynamic blacklist. Before the dynamic blacklist entry ages out, the STA cannot associate with the AP. 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 14-117 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 **14.4.22 dynamic-blacklist aging-time** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.

Related Topics

14.4.22 dynamic-blacklist aging-time

14.4.16 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

Copyright © Huawei Technologies Co., Ltd.

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 14-118 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
-------------------------------------------------------------
0          0021-1111-2222
-------------------------------------------------------------
Total: 1
```

Table 14-119 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 **14.4.40 sta-mac** command.

Related Topics

14.4.40 sta-mac

Copyright © Huawei Technologies Co., Ltd.

14.4.17 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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.4.55 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 detcted 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 14-120 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.

 Copyright © Huawei Technologies Co., Ltd.

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	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 14-121 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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.
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

14.4.55 wids attack detect enable

14.4.18 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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.4.55 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
------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-122 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 WPAI authentication mode
Total	Total number of attacks detected.

Related Topics

14.4.55 wids attack detect enable

 Copyright © Huawei Technologies Co., Ltd.

14.4.19 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

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, information about the detected attacking devices is saved in the attacking device list. If an attacking device no longer launches an attack, the device is removed from the attacking device list and saved to the historical attacking device list. You can run the **display wlan ids attack-history** command to check historical records about the attacking devices detected.

Prerequisites

The attack detection functions of all types have been enabled using the **14.4.55 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 14-123 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.

 Copyright © Huawei Technologies Co., Ltd.

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

14.4.55 wids attack detect enable

14.4.20 display wlan ids dynamic-blacklist

Function

The **display wlan ids dynamic-blacklist** command displays information about devices in the dynamic blacklist.

Format

display wlan ids dynamic-blacklist { **all** | **ap-id** *ap-id* | **ap-name** *ap-name* | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all devices in the dynamic blacklist.	-
ap-id *ap-id*	Displays information about attacking devices detected by the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about attacking devices detected by the AP with a specified name.	The AP name must exist.
mac-address *mac-address*	Displays information about attacking devices with a specified MAC address.	The MAC address must exist.

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An AP uses attack detection and dynamic blacklist functions to add a detected attacking 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 ids dynamic-blacklist** command to view information about devices in the dynamic blacklist.

Prerequisites

- The dynamic blacklist function has been enabled using the **14.4.23 dynamic-blacklist enable** command.
- The attack detection functions of all types have been enabled using the **14.4.55 wids attack detect enable** command.

Example

Display information about all devices in the dynamic blacklist.

```
<Huawei> display wlan ids dynamic-blacklist all
#AP: Number of monitor APs that have detected the device
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
--------------------------------------------------------------------------------
MAC address       Last detected time     Reason   #AP
--------------------------------------------------------------------------------
0020-1408-019f    2014-11-20/11:15:53    act      1
00bc-71b7-171f    2014-11-20/11:15:53    act      1
00d5-5862-641d    2014-11-20/11:15:43    pbr      1
--------------------------------------------------------------------------------
Total: 3, printed: 3
```

Table 14-124 Description of the **display wlan ids dynamic-blacklist all** command output

Item	Description
MAC address	MAC address of the device in the dynamic blacklist.
Last detected time	Latest time of device attack detection.
Reason	Reason why the device is added to the dynamic blacklist. The values here are the acronyms of attack types. For details, see **14.4.17 display wlan ids attack-detected**.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
#AP	Number of the AP that detects the device and adds it to the dynamic blacklist.

Display information about all devices added to the dynamic blacklist by AP **huawei**.

```
<Huawei> display wlan ids dynamic-blacklist ap-name huawei
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
--------------------------------------------------------------------------------
MAC address       Last detected time     Reason
--------------------------------------------------------------------------------
0020-1408-019f    2014-11-20/11:15:53    act
00bc-71b7-171f    2014-11-20/11:15:53    act
00d5-5862-641d    2014-11-20/11:15:43    pbr
--------------------------------------------------------------------------------
Total: 3, printed: 3
```

Display information about specified devices in the dynamic blacklist.

```
<Huawei> display wlan ids dynamic-blacklist mac-address e468-a350-8b3d
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
----------------------------------------------------------------
 Last detected time    Reason
----------------------------------------------------------------
 2014-11-20/11:15:53   act
 2014-11-20/11:15:53   act
 2014-11-20/11:15:43   pbr
----------------------------------------------------------------
Total: 3, printed: 3
```

Table 14-125 Description of the **display wlan ids dynamic-blacklist mac-address** command output

Item	Description
Last detected time	Last time when the device is detected.
Reason	Reason why the device is added to the dynamic blacklist.

Related Topics

14.4.23 dynamic-blacklist enable

14.4.55 wids attack detect enable

 Copyright © Huawei Technologies Co., Ltd.

14.4.21 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 (?) or spaces, 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
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 14-126 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.

14.4.22 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name huawei
[Huawei-wlan-ap-system-prof-huawei] dynamic-blacklist aging-time 300
```

Related Topics

14.4.23 dynamic-blacklist enable

14.4.23 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

 Copyright © Huawei Technologies Co., Ltd.

undo dynamic-blacklist enable

Parameters

None

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **dynamic-blacklist enable** command to enable the dynamic blacklist function. When detecting flood attacks or brute force password cracking attacks from a device, an AP reports the device to the AC, and the AC adds the device to a dynamic blacklist. Any packets sent from the device are rejected until the dynamic blacklist entry ages.

An AP can use the dynamic blacklist to filter out the blacklisted wireless devices to avoid malicious attacks.

Follow-up Procedure

Run the **14.4.22 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 ac
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] dynamic-blacklist enable
```

Related Topics

14.4.22 dynamic-blacklist aging-time

14.4.24 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 60 seconds.

Copyright © Huawei Technologies Co., Ltd.

Format

flood-detect interval *interval*

undo flood-detect interval

Parameters

Parameter	Description	Value
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 **14.4.23 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

Set the flood attack detection interval to 120s.

```
<Huawei> system-view
[Huawei] wlan ac
[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
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.25 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 a attack source launches attacks repeatedly, a large number of repetitive 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.

 Copyright © Huawei Technologies Co., Ltd.

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 **14.4.23 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 ac
[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

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.26 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 300 seconds.

Format

flood-detect threshold *threshold*

undo flood-detect threshold

Parameters

Parameter	Description	Value
threshold	Specifies the flood attack detection threshold.	The value is an integer that ranges from 1 to 1000.

 Copyright © Huawei Technologies Co., Ltd.

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 **14.4.23 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

Set the flood attack detection threshold to 350.

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.27 reset wlan ids attack-detected

Function

The **reset wlan ids attack-detected** command deletes information about the attacking devices detected.

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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

14.4.17 display wlan ids attack-detected

14.4.28 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

14.4.18 display wlan ids attack-detected statistics

 Copyright © Huawei Technologies Co., Ltd.

14.4.29 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

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, historical records 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-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

14.4.19 display wlan ids attack-history

14.4.30 reset wlan ids dynamic-blacklist

Function

The **reset wlan ids dynamic-blacklist** command deletes information about devices in the dynamic blacklist.

Format

reset wlan ids 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.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset wlan ids dynamic-blacklist** command is applicable to the following scenarios:

- To re-collect the dynamic blacklist information, run the **reset wlan ids dynamic-blacklist all** command to delete all information in the dynamic blacklist. After that, the AC re-collects the information.
- To remove an authorized device from the dynamic blacklist, run the **reset wlan ids 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 ids 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 ids dynamic-blacklist mac-address 78ac-c0c1-c1fc
```

14.4.31 security dot1x

Function

The **security dot1x** 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** } **dot1x** { **aes** | **tkip** | **aes-tkip** }

undo security

 Copyright © Huawei Technologies Co., Ltd.

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.	-
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

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 802.1X authentication, run the **security dot1x** command. If multiple types of user terminals are available, you can configure the WPA-WPA2 and TKIP-CCMP security policy for authentication and data encryption.

NOTE

The following terminals do not support the WPA2 802.1X authentication and cannot access the AP. You must configure other security policies for the terminals.

- 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure WPA authentication (802.1X and TKIP encryption).

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa dot1x tkip
```

Configure WPA2 authentication (802.1X and TKIP encryption).

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa2 dot1x tkip
```

Configure WPA-WPA2 authentication (802.1X authentication and AES-TKIP encryption).

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa-wpa2 dot1x aes-tkip
```

14.4.32 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** }

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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
key-value	Specifies a password in cipher text.	The value is of 8 to 63 ASCII characters in plain text, 64 hexadecimal characters in plain text, or 48 or 68 or 88 or 108 characters in cipher text. The question mark (?) is supported, which you can enter by pressing **Ctrl+T**. In **pass-phrase** mode, the key must be a combination of at least two of the following: lowercase letters, uppercase letters, digits, 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

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.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

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.

Example

Configure WPA pre-shared key authentication and the authentication key.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa psk pass-phrase abcdfffffgF aes
```

Configure WPA2 pre-shared key authentication and the authentication key.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa2 psk pass-phrase abcdfffffgF aes
```

Configure WPA-WPA2 pre-shared key authentication and TKIP-CCMP encryption.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa-wpa2 psk pass-phrase abcdfffffgF aes-tkip
```

14.4.33 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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 recommend.	-
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. The cipher-text characters must be a combination of at least two of the following: lowercase letters, uppercase letters, digits, and special characters.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

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.

 Copyright © Huawei Technologies Co., Ltd.

- 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.

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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wapi psk pass-phrase testpasswordF
```

14.4.34 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.	-
share-key	Sets the WEP authentication mode to share-key authentication.	-

Views

Security profile view

 Copyright © Huawei Technologies Co., Ltd.

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 14-127 Comparison between open system authentication and share-key authentication

Authentication Mode	Advantage	Disadvantage
open	Wireless devices can connect to a network without authentication.	STA identities are not checked, bringing security risks.
share-key	A share-key is used to enhance security.	• 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 authentication mode is set to **share-key**, run the **14.4.54 wep key** command to configure a share-key.
- If the authentication mode is set to **open**, the WEP share-key configured in the profile cannot take effect.
- Each AP can have at most four key indexes configured. The key indexes used by different VAPs cannot be the same. If a key index takes effect on a VAP, the key index cannot be applied to other VAPs.
- The system displays the message only when the security profile has been bound to the other profiles.

Example

Create security profile **p1** and set the authentication mode to **share-key**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wep share-key
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.4.54 wep key

14.4.35 security-profile

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** and **default-wds** 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 begin or end with double quotation marks (" ").
all	Deletes all security profiles. **NOTE** Security profiles **default** and **default-wds** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1]
```

Related Topics

14.4.13 display security-profile

14.4.36 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] vap-profile name ChinaNet
[Huawei-wlan-vap-prof-ChinaNet] security-profile security-profile1
```

Related Topics

14.4.35 security-profile

14.1.127 display vap-profile

14.4.37 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

 Copyright © Huawei Technologies Co., Ltd.

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 repetitive 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 ac
[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

14.4.55 wids attack detect enable

14.4.38 sta-access-mode

Function

The **sta-access-mode** command binds STA blacklist and STA whitelist profiles to AP system profiles.

The **undo sta-access-mode** command unbinds STA blacklist and STA whitelist profiles from AP system profiles.

By default, no STA blacklist and STA whitelist profiles are bound to an AP system profile.

Format

sta-access-mode { **blacklist** | **whitelist** } *profile-name*

undo sta-access-mode

 Copyright © Huawei Technologies Co., Ltd.

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

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

STA blacklists and whitelists configured by using the **14.4.40 sta-mac** command take effect only after the STA blacklist and whitelist profiles are bound to 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.

- AP system profile: The STA blacklist and whitelist take effect on the corresponding AP.

Example

Bind the STA blacklist profile **sta-blacklist-profile1** to the AP system profile **ap-system-profile1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system-profile1
[Huawei-wlan-ap-system-prof-ap-system-profile1] sta-access-mode blacklist sta-blacklist-profile1
```

Related Topics

14.4.40 sta-mac

14.4.39 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.

Copyright © Huawei Technologies Co., Ltd.

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 begin 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 an AP system profile using the **14.4.38 sta-access-mode** command.

If a STA is added to the blacklist, the system automatically disconnects the STA.

Example

Create the STA blacklist profile **sta-blacklist-profile1**.

```
<Huawei> system-view
[Huawei] wlan ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] sta-blacklist-profile name sta-blacklist-profile1
[Huawei-wlan-blacklist-prof-sta-blacklist-profile1]
```

Related Topics

14.4.38 sta-access-mode
14.4.14 display sta-blacklist-profile

14.4.40 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*

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.
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.

 Copyright © Huawei Technologies Co., Ltd.

If a STA is added to the blacklist, the system automatically disconnects the STA.

Example

Add MAC address 2C27-D720-746B of a STA to blacklist **huawei**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-blacklist-profile name sta-blacklist-profile1
[Huawei-wlan-blacklist-prof-sta-blacklist-profile1] sta-mac 2C27-D720-746B
```

Related Topics

14.4.14 display sta-blacklist-profile

14.4.16 display sta-whitelist-profile

14.4.41 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 begin or end with double quotation marks (" ").
all	Deletes all STA whitelist profiles.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

The configured whitelist takes effect only after the STA whitelist profile is bound to an AP system profile using the **14.4.38 sta-access-mode** command.

If the configured whitelist takes effect, only STAs in the whitelist can access the WLAN.

Example

Create the STA whitelist profile **sta-whitelist-profile1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-whitelist-profile name sta-whitelist-profile1
[Huawei-wlan-whitelist-prof-sta-whitelist-profile1]
```

Related Topics

14.4.38 sta-access-mode

14.4.16 display sta-whitelist-profile

14.4.42 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.

Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi asu ip 10.164.10.10
```

14.4.43 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** }

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Set the interval for updating a BK to 10000s and the BK lifetime percentage to 80%.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi bk-update-interval 10000
[Huawei-wlan-sec-prof-p1] wapi bk-threshold 80
```

14.4.44 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*

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi cert-retrans-count 5
```

14.4.45 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** }

 Copyright © Huawei Technologies Co., Ltd.

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.	-
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 (?) or spaces, 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.

 Copyright © Huawei Technologies Co., Ltd.

- 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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi import certificate ac format pem file-name flash:/local_ac.cer
Warning: This action may cause service interruption. Continue?[Y/N]y
```

14.4.46 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.	-

Parameter	Description	Value
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 (?) or spaces, and cannot start or end with double quotation marks (" ") or spaces.
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**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi import private-key format pem file-name flash:/ac_key.key
Warning: This action may cause service interruption. Continue?[Y/N]y
```

Related Topics

14.4.13 display security-profile

14.4.47 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 **14.4.48 wapi msk** and **14.4.51 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.

Copyright © Huawei Technologies Co., Ltd.

- 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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi usk key-update time-based
```

Related Topics

14.4.48 wapi msk

14.4.51 wapi usk

14.4.48 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 **14.4.47 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.

Copyright © Huawei Technologies Co., Ltd.

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 ac
[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

14.4.47 wapi key-update

14.4.49 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi sa-timeout 100
```

14.4.50 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi source interface Vlanif 100
```

 Copyright © Huawei Technologies Co., Ltd.

14.4.51 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 **14.4.47 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 ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[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

14.4.47 wapi key-update

14.4.52 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 repetitive 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.

Copyright © Huawei Technologies Co., Ltd.

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 ac
[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

14.4.55 wids attack detect enable

14.4.53 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

 Copyright © Huawei Technologies Co., Ltd.

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. If a key index takes effect on a VAP, the key index cannot be applied to other VAPs.
- 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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wep default-key 1
```

Related Topics

14.4.54 wep key

14.4.54 wep key

Function

The **wep key** command sets a WEP key.

The **undo wep key** command deletes the specified key.

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

Format

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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
wep-104	Configures WEP-104 authentication.	-
wep-128	Configures WEP-128 authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number.	-

 Copyright © Huawei Technologies Co., Ltd.

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. Here, ASCII characters contain only digits or letters. In **pass-phrase** mode, the key must be a combination of at least two of the following: lowercase letters, uppercase letters, and digits.

Views

Security profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

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.

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 ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wep key 1 wep-128 hex
12345678123456781234567812345678a
Warning: This action may cause service interruption. Continue?
[Y/N]y
Info: This operation may take a few seconds, please wait.done.
```

Related Topics

14.4.53 wep default-key

14.4.55 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** }

 Copyright © Huawei Technologies Co., Ltd.

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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.4.23 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 ac
[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

14.4.23 dynamic-blacklist enable

14.4.56 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 **14.4.8 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** }

Copyright © Huawei Technologies Co., Ltd.

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 begin 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 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 attacks in the profile.

Follow-up Procedure

Run the **14.4.57 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 ac
[Huawei-wlan-view] wids-profile name office
[Huawei-wlan-wids-prof-office]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.4.57 wids-profile (AP group view and AP view)

14.4.57 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 **14.4.56 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 ac
[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 ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[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

14.4.56 wids-profile (WLAN view)

14.4.58 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 begin or end with double quotation marks (" ").
all	Deletes all WIDS spoof SSID profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Follow-up Procedure

Run the **14.4.59 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 ac
[Huawei-wlan-view] wids-spoof-profile name office
[Huawei-wlan-wids-spoof-office]
```

Related Topics

14.4.59 wids-spoof-profile (WIDS profile view)

14.4.59 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

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After you create a WIDS spoof SSID profile using the **14.4.58 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 ac
[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

14.4.58 wids-spoof-profile (WLAN view)
14.4.56 wids-profile (WLAN view)

14.4.60 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

 Copyright © Huawei Technologies Co., Ltd.

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 terminals may go offline due to individual problems.

Follow-up Procedure

Run the **14.4.61 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 ac
[Huawei-wlan-view] security-profile name huawei
[Huawei-wlan-sec-prof-huawei] wpa ptk-update enable
```

Related Topics

14.4.61 wpa ptk-update ptk-update-interval

14.4.61 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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.4.60 wpa ptk-update enable** command.

Example

Set the periodic PTK update interval to 50,000 seconds.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name huawei
[Huawei-wlan-sec-prof-huawei] wpa ptk-update ptk-update-interval 50000
```

Related Topics

14.4.60 wpa ptk-update enable

14.5 WLAN WDS Configuration Commands

14.5.1 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] dhcp trust port
```

Related Topics

14.5.20 wds-profile

14.5.2 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

 Copyright © Huawei Technologies Co., Ltd.

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 14-128 Description of the **display references wds-profile name** command output

Parameter	Description
Reference type	Type of the profile to which the WDS profile is bound.
Reference name	Name of the profile to which the WDS profile is bound. • Run the **14.5.21 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 **14.5.22 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

14.5.4 display wds-profile

14.5.21 wds-profile radio

14.5.22 wds-profile (AP group radio view or AP radio view)

Copyright © Huawei Technologies Co., Ltd.

14.5.3 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 14-129 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.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Reference name	Name of the profile to which the WDS whitelist profile is bound. Run the **14.5.24 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

14.5.5 display wds-whitelist-profile
14.5.23 wds-whitelist-profile
14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)

14.5.4 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.

Copyright © Huawei Technologies Co., Ltd.

Example

Display reference information about all WDS profiles.

```
<Huawei> display wds-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
default                          0
test                            2
--------------------------------------------------------------------------------
Total: 2
```

Table 14-130 Description of the **display wds-profile all** command output

Item	Description
Profile name	WDS profile name. To create a WDS profile, run the **14.5.20 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
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
--------------------------------------------------------------------------------
```

Table 14-131 Description of the **display wds-profile name** command output

Item	Description
WDS name	WDS name. To set a WDS name, run the **14.5.19 wds-name** command.
WDS work mode	WDS working mode. To set the WDS working mode, run the **14.5.18 wds-mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Security profile	Security profile bound to a WDS profile. To bind a security profile to a WDS profile, run the **14.5.12 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 **14.5.1 dhcp trust port (WDS profile view)** command.
Tagged vlan	VLAN configured in a WDS profile. To configure a VLAN in a WDS profile, run the **14.5.16 vlan tagged (WDS profile view)** command.
Priority map trust	Priority mapping trusted by the WDS air interface. To configure the parameter, run the **14.5.11 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 **14.5.10 priority-map dscp (WDS profile view)** command.

Related Topics

14.5.1 dhcp trust port (WDS profile view)
14.5.12 security-profile (WDS profile view)
14.5.16 vlan tagged (WDS profile view)
14.5.18 wds-mode
14.5.19 wds-name

Copyright © Huawei Technologies Co., Ltd.

14.5.5 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
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-132 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 **14.5.23 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 14-133 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 **14.5.9 peer-ap mac (WDS whitelist profile view)** command.

Related Topics

14.5.23 wds-whitelist-profile

14.5.9 peer-ap mac (WDS whitelist profile view)

14.5.6 display wds vap

Function

The **display wds vap** command displays information about a WDS VAP.

Copyright © Huawei Technologies Co., Ltd.

Format

display wds vap { **ap-group** *ap-group-name* | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] } [**wds-name** *wds-name*]

display wds vap { **all** | **wds-name** *wds-name* }

Parameters

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

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds vap** command to display information about a WDS VAP.

Example

Display information about all WDS VAPs.

```
<Huawei> display wds vap all
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name       RfID WID        WDS name            BSSID         WDS links
--------------------------------------------------------------------------------
1     AP2           0  14         wds                 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
```

 Copyright © Huawei Technologies Co., Ltd.

```
--------------------------------------------------------------------------------
Total: 4
```

Table 14-134 Description of the **display wds vap** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
WID	WLAN ID of a VAP.
WDS name	WDS name. To set a WDS name, run the **14.5.19 wds-name** command.
BSSID	MAC address of a VAP.
WDS links	Number of WDS links.

Related Topics

14.5.7 display wlan wds link

14.5.19 wds-name

14.5.7 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.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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(Ch0~2: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 14-135 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.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
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(Ch0~2:dB)	SNR of each spatial stream of a WDS link.

Related Topics

14.5.6 display wds vap

14.5.8 mode (AP wired port profile view)

Function

The **mode** command sets the working mode for an AP's wired interface.

The **undo mode** command restores the default working mode of an AP's wired interface.

By default, the GigabitEthernet interface of a common AP works in **root** mode, the Ethernet interface in **endpoint** mode, and the Eth-trunk interface in **root** mode.

NOTE

You cannot change the working mode of wired interfaces on the 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
endpoint	Sets the working mode of an AP's wired interface to endpoint, which can connect to a computer or switch.	-
middle	Sets the working mode of an AP wired interface to middle, which can connect to an RRU.	-

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 RRUs through downlink GigabitEthernet interfaces, the working mode of the downlink GigabitEthernet interfaces must be set to **middle**.

Configuration Impact

The AP's wired interface supports user isolation in endpoint mode, but not in root mode.

If the working mode of an AP's wired interface is set to **root** in the AP wired port profile, you cannot set the **vlan pvid** *vlan-id*. In turn, if you set the **vlan pvid** *vlan-id*, you cannot set the working mode of the AP's wired interface to **root**.

Example

Set the working mode of the AP's wired interface GE0 to **endpoint**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name ap-group1
[Huawei-wlan-ap-group-ap-group1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] wired-port-profile name wired
[Huawei-wlan-wired-port-wired] mode endpoint
[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

14.1.240 wired-port-profile (WLAN view)

14.5.9 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[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

14.5.23 wds-whitelist-profile

14.5.10 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 14-136 describes the mapping from DSCP priorities to 802.11e user priorities by default.

Table 14-136 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] priority-map dscp 0 to 6 dot11e 0
```

Related Topics

14.5.11 priority-map trust (WDS profile view)

14.5.11 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.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the WDS air interface to trust the mapping from 802.1p priorities to 802.11e user priorities.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] priority-map trust dot1p
```

Related Topics

14.5.10 priority-map dscp (WDS profile view)

14.5.12 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 and be configured with the security policy WPA2+PSK+AES.

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

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

Currently, the WDS profile supports only the security policy WPA2+PSK+AES. 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 ac
[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
```

Related Topics

14.4.35 security-profile

14.5.20 wds-profile

14.5.13 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.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
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.

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 ac
[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
[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

14.1.240 wired-port-profile (WLAN view)

14.5.14 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.

 Copyright © Huawei Technologies Co., Ltd.

Format

user-isolate l2

undo user-isolate

Parameters

Parameter	Description	Value
l2	Specifies Layer 2 user isolation.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The user isolation function prevents users in the same traffic profile from communicating with each other. All user traffic in the traffic profile is forwarded by the gateway. Therefore, this function ensures communication security on wired interfaces and allows uniform charging for users.

You can run the **user-isolate** command to enable user isolation on a traffic profile.

Example

Enable Layer 2 user isolation in traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] user-isolate l2
Warning: This action may cause service interruption. Continue?[Y/N]y
```

14.5.15 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*

 Copyright © Huawei Technologies Co., Ltd.

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 AP's management VLAN is configured using the **management-vlan** *vlan-id* command, packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in untagged mode using the **vlan untagged** *vlan-id* command, the packets sent from the AP's wired interface are not tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in tagged mode using the **vlan tagged** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the PVID of the AP's wired interface is set to the management VLAN ID using the **vlan pvid** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.

Precautions

Eth-Trunk member interfaces do not support PVID setting.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[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
[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

14.1.240 wired-port-profile (WLAN view)

14.5.16 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** }

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] vlan tagged 3 to 6 10 12
```

Related Topics

14.5.20 wds-profile

 Copyright © Huawei Technologies Co., Ltd.

14.5.17 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 is added to VLAN 1 in untagged mode.

NOTE

An AP's wired interface can be added to a maximum of 256 VLANs.

Format

vlan { **tagged** | **untagged** } { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan { **all** | *vlan-id1* [**to** *vlan-id2*] &<1-10> }

Parameters

Parameter	Description	Value
tagged	Adds a wired interface to a VLAN in tagged mode.	-
untagged	Adds a wired interface to a VLAN in untagged mode.	-

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 AP's management VLAN is configured using the **management-vlan** *vlan-id* command, packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in untagged mode using the **vlan untagged** *vlan-id* command, the packets sent from the AP's wired interface are not tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in tagged mode using the **vlan tagged** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the PVID of the AP's wired interface is set to the management VLAN ID using the **vlan pvid** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.

Configuration Impact

Eth-Trunk member interfaces cannot be added to VLANs.

Example

Set the working mode of the AP's 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 ac
[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
[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

14.1.240 wired-port-profile (WLAN view)

14.5.18 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** }

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] wds-mode middle
```

Related Topics

14.5.20 wds-profile

14.5.19 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**.

 Copyright © Huawei Technologies Co., Ltd.

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 **14.5.19 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 ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] wds-name bridge
```

Related Topics

14.5.20 wds-profile

14.5.20 wds-profile

Copyright © Huawei Technologies Co., Ltd.

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 begin 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 **14.5.19 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**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] wds-name bridge
```

Related Topics

14.5.19 wds-name

14.5.21 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Bind the WDS profile **test** to radio **0** of APs in the AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] wds-profile test radio 0
```

Related Topics

14.5.20 wds-profile

14.5.22 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

 Copyright © Huawei Technologies Co., Ltd.

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 **14.5.21 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 ac
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] radio 0
[Huawei-wlan-group-radio-group1/0] wds-profile test
```

Related Topics

14.5.20 wds-profile

14.5.21 wds-profile radio

14.5.23 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* }

 Copyright © Huawei Technologies Co., Ltd.

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 begin 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 **14.5.9 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 ac
[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

14.5.9 peer-ap mac (WDS whitelist profile view)

14.5.20 wds-profile

14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)

Copyright © Huawei Technologies Co., Ltd.

14.5.24 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[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

14.5.20 wds-profile

14.5.23 wds-whitelist-profile

14.6 WLAN Reliability Commands

14.6.1 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ac protect cold-backup kickoff-station
```

Related Topics

14.6.6 display ac protect

14.6.2 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

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ac protect enable
Warning: This operation maybe cause AP reset, continue?[Y/N]:y
```

Related Topics

14.6.6 display ac protect

14.6.3 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ac protect priority 3
```

Related Topics

14.6.6 display ac protect

14.6.7 priority

14.6.4 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

 Copyright © Huawei Technologies Co., Ltd.

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.

Example

Set the standby AC IP address to 10.33.12.56 in the WLAN view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ac protect protect-ac 10.33.12.56
```

Related Topics

14.6.6 display ac protect
14.6.8 protect-ac

14.6.5 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.

 Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ac protect restore disable
```

Related Topics

14.6.6 display ac protect

14.6.6 display ac protect

Function

The **display ac protect** command displays AC dual-link backup configuration.

 Copyright © Huawei Technologies Co., Ltd.

Format

display ac protect

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays 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
-------------------------------------------------------------
```

Table 14-137 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 **14.6.2 ac protect enable** command.
Protect AC	Standby AC IP address. To configure the parameter, run the **14.6.4 ac protect protect-ac** command.

Copyright © Huawei Technologies Co., Ltd.

Priority	Priority of the local AC. To configure the parameter, run the **14.6.3 ac protect priority** command.
Protect restore	Whether global revertive switching is enabled on the AC. To configure the parameter, run the **14.6.5 ac protect restore disable** command.
Coldbackup kickoff station	Whether to enable the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured. To configure the parameter, run the **14.6.1 ac protect cold-backup kickoff-station** command.

Related Topics

14.6.1 ac protect cold-backup kickoff-station
14.6.2 ac protect enable
14.6.3 ac protect priority
14.6.4 ac protect protect-ac
14.6.5 ac protect restore disable

14.6.7 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

Copyright © Huawei Technologies Co., Ltd.

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 ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] priority 3
```

Related Topics

14.1.98 display ap-system-profile

 Copyright © Huawei Technologies Co., Ltd.

14.6.8 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.

Example

Set the standby AC's IP address to 10.3.3.3 in the AP system profile view.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[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

14.1.98 display ap-system-profile

 Copyright © Huawei Technologies Co., Ltd.