H3C MSR Router Series

Comware 5 WLAN Command Reference

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: MSR-CMW520-R2516
Document version: 20180820-C-1.13

Preface

This command reference describes the WLAN configuration commands.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.
- Documentation feedback.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the routers.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

WLAN interface configuration commands

The terms *AP* and *fat AP* in this document refer to MSR800, MSR 900, MSR900-E, MSR 930, and MSR 20-1X routers with IEEE 802.11b/g and MSR series routers installed with a SIC WLAN module.

WLAN is not available on the following routers:

- MSR 2600.
- MSR 30-11.
- MSR 30-11E.
- MSR 30-11F.
- MSR3600-51F.

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Views

WLAN BSS interface view, WLAN Ethernet interface view, WLAN radio interface view

Default command level

2: System level

Parameters

bandwidth-value: Expected bandwidth in the range of 1 to 4294967295 kbps.

Usage guidelines

Obtain the expected bandwidth by using a third-party software to query MIB node ifspeed.

The network management station uses the expected bandwidth to monitor the interface bandwidth and does not affect the actual interface bandwidth.

Examples

Set the expected bandwidth of a WLAN BSS interface to 10000 kbps.

```
<Sysname> system-view
[Sysname] interface wlan-bss 1
[Sysname-WLAN-BSS1] bandwidth 10000
```

default

Use **default** to restore the default settings for an interface.

Syntax

default

Views

WLAN BSS interface view, WLAN Ethernet interface view, WLAN radio interface view

Default command level

2: System level

Usage guidelines

This command might fail to restore the default settings for some commands because of command dependencies and system restrictions. You can use the **display this** command in interface view to check for these commands, and perform their **undo** forms or follow the command reference to individually restore their default settings. Follow the instructions in the error message to resolve the problem if the restoration attempt fails.

The **default** command might interrupt ongoing network services. Be fully aware of the impacts of this command when you perform it on a live network.

Examples

Restore the default settings of WLAN BSS interface 1.

```
<Sysname> system-view
[Sysname] interface wlan-bss 1
[Sysname-WLAN-BSS1] default
This command will restore the default settings. Continue? [Y/N]:y
```

description

Use **description** to set the description for the current interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description for an interface is *interface-name* + **Interface**.

Views

WLAN BSS interface view, WLAN Ethernet interface view, WLAN radio interface view

Default command level

2: System level

Parameters

text: Description for the current interface, a string of 1 to 80 characters. The device supports the following types of characters or symbols: standard English characters (numbers and case-sensitive letters), special English characters, spaces, and other characters or symbols that conform to the Unicode standard.

Usage guidelines

An interface description can be the mixture of English characters and other Unicode characters. The mixed description cannot exceed the specified length.

To use a type of Unicode characters or symbols in an interface description, you must install the corresponding IME and log in to the device through remote login software that supports this character type.

Each Unicode character or symbol (non-English characters) takes the space of two regular characters. When the length of a description string reaches or exceeds the maximum line width on the terminal software, the software starts a new line, possibly breaking a Unicode character into two parts. As a result, garbled characters might be displayed at the end of a line.

Examples

Set the description for WLAN radio 2/0 to **WLAN radio2 Interface**.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] description WLAN-Radio2 Interface
```

display interface WLAN BSS

Use **display interface wlan-bss** to display information about the specified WLAN BSS interface or all WLAN BSS interfaces if no WLAN BSS interface is specified.

Syntax

display interface [**wlan-bss**] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display interface wlan-bss *interface-number* [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

interface-number: Specifies a WLAN BSS interface by its number.

brief: Displays brief interface information. If you do not provide this keyword, the command displays detailed interface information.

down: Displays down interface information and the cause. If you do not provide this keyword, the command output is not filtered based on the down interface status.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

- If you do not provide the **wlan-bss** keyword, the command displays information about all interfaces on the device.
- If you provide the **wlan-bss** keyword, and do not provide the interface-number argument, the command displays information about all WLAN BSS interfaces.

Examples

Display information about the interface WLAN-BSS 1. (Assume that the interface does not support traffic statistics collection.)

```
<Sysname> display interface wlan-bss 1
 WLAN-BSS1 current state: DOWN
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-0000-0000
 Description: WLAN-BSS1 Interface
 PVID: 1
 Port link-type: access
```

```
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1
 Port priority: 0
Last clearing of counters:  Never
```

Table 1 Command output

Field	Description
WLAN-BSS1 current state	Physical link state of a WLAN BSS interface.
IP Packet Frame Type	Output frame encapsulation type.
Hardware Address	MAC address of output frames.
Description	Description of the interface.
PVID	Default VLAN ID of the interface.
Port link-type	Port link type, which can be access or hybrid.
Tagged VLAN ID	VLANs whose packets are sent through the port with VLAN tag kept.
Untagged VLAN ID	VLANs whose packets are sent through the port with VLAN tag stripped off.
Last clearing of counters: Never	Time when the **reset counts interface** command was last used to clear statistics on the interface. **Never** indicates that the **reset counts interface** command was never used after the device was started.

display interface wlan-ethernet

Use **display interface wlan-ethernet** to display information about a WLAN Ethernet interface.

Syntax

display interface [**wlan-ethernet**] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display interface wlan-ethernet *interface-number* [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

interface-number: Specifies a WLAN Ethernet interface by its number.

brief: Displays brief interface information. If you do not provide this keyword, the command displays detailed interface information.

down: Displays down interface information and the cause. If you do not provide this keyword, the command output is not filtered based on the down interface status.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

If you do not specify the **wlan-ethernet** keyword, the command displays information about all interfaces on the device.

If you specify the **wlan-ethernet** keyword, and do not specify the *interface-number* argument, the command displays information about all WLAN Ethernet interfaces.

Examples

Display information about the interface WLAN-Ethernet 1. (Assume that the interface does not support traffic statistics collection.)

```
<Sysname> display interface wlan-ethernet 1
WLAN-Ethernet1 current state: DOWN
Line protocol current state: DOWN
Description: WLAN-Ethernet1 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 0000-0000-0000
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 0000-0000-0000
Last clearing of counters:  Never
```

Table 2 Command output

Field	Description
WLAN-Ethernet1 current state	Physical link state of a WLAN Ethernet interface: • **DOWN (Administratively)**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively brought up but is physically shut down (line failure or no physical connection). • **UP**—The interface is both administratively and physically brought up.
Line protocol current state	Link layer state of the interface. When the interface is physically down, the field is displayed as DOWN. When the interface is physically up, the field is displayed as UP.
Description	Description of the interface.
The Maximum Transmit Unit	Maximum transmit unit (MTU) of the interface.
Internet protocol processing	IP packet processing. disabled means IP packets cannot be processed. When you configure the IP address for an interface, the field is changed to Internet Address is.
Last clearing of counters: Never	Time when the **reset counts interface** command was last used to clear statistics on the interface. **Never** indicates that the **reset counts interface** command was never used after the device was started.

display interface wlan-radio

Use **display interface wlan-radio** to display information about a WLAN radio interface.

Syntax

display interface [**wlan-radio**] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

display interface wlan-radio *interface-number* [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

interface-number: Specifies a WLAN radio interface by its number.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

down: Displays down interface information and the cause. If you do not specify this keyword, the command output is not filtered based on the down interface status.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

If you do not specify the **wlan-radio** keyword, the command displays information about all interfaces on the device.

If you specify the **wlan-radio** keyword, and do not specify the *interface-number* argument, the command displays information about all WLAN radio interfaces.

Examples

Display information about the interface WLAN-Radio 2/0.

```
<Sysname> display interface WLAN-Radio 2/0
WLAN-Radio2/0 current state: UP
IP Packet Frame Type: PKTFMT_IEEE_802.11, Hardware Address: 000f-e2c0-0110
Description: WLAN-Radio2/0 Interface
Radio-type dot11g, channel auto, power(dBm) 23
Secondary channel offset: SCN, HT protection mode: no protection
Received: 0 authentication frames, 0 association frames
Sent out: 0 authentication frames, 0 association frames
Stations: 0 associating, 0 associated
 Input : 30007 packets, 1536614 bytes
        : 13565 unicasts, 520774 bytes
        : 16442 multicasts/broadcasts, 1015840 bytes
        : 0 fragmented
        : 5687 discarded, 263913 bytes
        : 0 duplicates, 3054 FCS errors
        : 2 decryption errors
 Output: 2032 packets, 468562 bytes
       : 7 unicasts, 1776 bytes
       : 312 multicasts/broadcasts, 40114 bytes
       : 1713 others, 426672 bytes
```

```
: 0 fragmented
: 0 discarded, 0 bytes
: 0 failed RTS, 335 failed ACK
: 334 transmit retries, 122 multiple transmit retries
```

Table 3 Command output

Field	Description
WLAN-Radio2/0 current state	Physical link state of the WLAN radio interface.
IP Packet Frame Type	Output frame encapsulation type.
Hardware Address	MAC address of the interface.
Description	Description of the interface.
Radio-type dot11g	WLAN protocol type used by the interface.
channel auto(11)	Channel used by the interface. The keyword auto means the channel is automatically selected and 11 is the number of the selected channel. If the channel is manually selected, the field will be displayed in the format of **channel** *configured-channel.*
power(dBm) 23	Transmit power of the interface (in dBm). The value 23 is the transmit power configured by the user. For more information about the **max-power** command, see *WLAN Command Reference*.
Secondary channel offset	Secondary channel information for 802.11n radio mode: • **SCA (Second Channel Above)**—The AP operates in 40 MHz bandwidth mode, and the secondary channel has a higher bandwidth than the primary channel. • **SCB (Second Channel Below)**—The AP operates in 40 MHz bandwidth mode, and the secondary channel has a lower bandwidth than the primary channel. • **SCN**—The AP operates in 20 MHz bandwidth mode.
HT protection mode	802.11n protection modes: • **no protection mode(0)**—The clients associated with the AP, and the wireless devices within the coverage of the AP operate in 802.11n mode, and all the clients associated with the AP operate in either 40 MHz or 20 MHz mode. • **Non-member mode(1)**—The clients associated with the AP operate in 802.11n mode, but non-802.11n wireless devices exist within the coverage of the AP. • **20 MHz mode(2)**—The radio mode of the AP is 40 MHz. The clients associated with the AP and the wireless devices within the coverage of the AP operate in 802.11n mode, and at least one 802.11n client operating in 20 MHz mode is associated with the radio of the AP. • **Non-HT mix mode(3)**—All situations except the above three.
Received: 0 authentication frames, 0 association frames	Received: Number of authentication frames, number of association frames.
Sent out: 0 authentication frames, 0 association frames	Sent out: Number of authentication frames, number of association frames.
Stations: 0 associating, 0 associated	Number of wireless users.
Input : 30007 packets, 1536614 bytes : 13565 unicasts, 520774 bytes	Input packet statistics of the interface: • Number of packets, number of bytes.

Field	Description
: 16442 multicasts/broadcasts, 1015840 bytes : 0 fragmented : 5687 discarded, 263913 bytes : 0 duplicates, 3054 FCS errors : 2 decryption errors	• Number of unicast packets, number of bytes of unicast packets. • Number of multicasts/broadcast packets, number of bytes of multicasts/broadcast packets. • Number of fragmented packets. • Number of discarded packets, number of discarded bytes. • Number of duplicate frames, number of FCS errors. • Number of encryption errors.
Output: 2032 packets, 468562 bytes : 7 unicasts, 1776 bytes : 312 multicasts/broadcasts, 40114 bytes : 1713 others, 426672 bytes : 0 fragmented : 0 discarded, 0 bytes : 0 failed RTS, 335 failed ACK : 334 transmit retries, 122 multiple transmit retries	Output packet statistics of the interface: • Number of packets (unicasts + multicasts/broadcasts + others), number of bytes. • Number of unicast packets, number of bytes of unicast packets. • Number of multicasts/broadcast packets, number of bytes of multicasts/broadcast packets. • Number of other types of packets, bytes. • Number of fragmented packets. • Number of discarded packets, number of discarded bytes. • Number of failed RTS packets, number of failed ACK packets. • Number of retransmitted frames, number of transmit retries.

interface wlan-bss

Use **interface wlan-bss** to enter WLAN BSS interface view. If the WLAN BSS interface identified by the *interface-number* argument does not exist, this command creates the WLAN BSS interface first.

Use **undo interface wlan-bss** to remove a WLAN BSS interface.

Syntax

interface wlan-bss *interface-number*

undo interface wlan-bss *interface-number*

Views

System view

Default command level

2: System level

Parameters

interface-number: Specifies a WLAN BSS interface by its number.

Examples

Create the WLAN BSS interface numbered 1.

```
<Sysname> system-view
[Sysname] interface wlan-bss 1
[Sysname-WLAN-BSS1]
```

interface wlan-ethernet

Use **interface wlan-ethernet** to enter WLAN Ethernet interface view. If the WLAN Ethernet interface identified by the *interface-number* argument does not exist, this command creates the WLAN Ethernet interface first.

Use **undo interface wlan-ethernet** to remove a WLAN Ethernet interface.

Syntax

interface wlan-ethernet *interface-number*

undo interface wlan-ethernet *interface-number*

Views

System view

Default command level

2: System level

Parameters

interface-number: Specifies a WLAN Ethernet interface by its number.

Examples

Create the WLAN Ethernet interface numbered 1.

```
<Sysname> system-view
[Sysname] interface wlan-ethernet 1
[Sysname-WLAN-Ethernet1]
```

interface wlan-radio

Use **interface wlan-radio** to enter WLAN radio interface view.

Syntax

interface wlan-radio *interface-number*

Views

System view

Default command level

2: System level

Parameters

interface-number: Specifies a WLAN radio interface by its number.

Examples

Enter WLAN-Radio 2/0 interface view.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0]
```

shutdown (WLAN radio interface view)

Use **shutdown** to shut down the current WLAN radio interface.

Use **undo shutdown** to bring up the current WLAN radio interface.

Syntax

shutdown

undo shutdown

Default

A WLAN radio interface is up.

Views

WLAN radio interface view

Default command level

2: System level

Examples

Shut down interface WLAN-Radio 2/0.

```
<Sysname>system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] shutdown
```

shutdown (WLAN BSS interface view)

Use **shutdown** to shut down the current WLAN BSS interface.

Use **undo shutdown** to bring up the current WLAN BSS interface.

Syntax

shutdown

undo shutdown

Default

A WLAN BSS interface is up.

Views

WLAN BSS interface view

Default command level

2: System level

Usage guidelines

After a WLAN BSS interface is shut down, the connection between the interface and the wireless device will be torn down.

Examples

Shut down interface WLAN-BSS 1.

```
<Sysname>system-view
[Sysname] interface wlan-bss 1
[Sysname-WLAN-Bss1] shutdown
```

WLAN access configuration commands

The terms *AP* and *fat AP* in this document refer to MSR800, MSR 900, MSR900-E, MSR 930, and MSR 20-1X routers with IEEE 802.11b/g and MSR series routers installed with a SIC WLAN module.

WLAN is not available on the following routers:

- MSR 2600.
- MSR 30-11.
- MSR 30-11E.
- MSR 30-11F.
- MSR3600-51F.

802.11 MAC configuration commands

a-mpdu enable

Use **a-mpdu enable** to enable the Aggregated MAC Protocol Data Unit (A-MPDU) function for the radio.

Use **undo a-mpdu enable** to disable the A-MPDU function for the radio.

Syntax

a-mpdu enable

undo a-mpdu enable

Default

The A-MPDU function is enabled.

Views

WLAN-radio interface view

Default command level

2: System level

Usage guidelines

This command is only effective on 802.11n radios.

If you change the radio type of an 802.11n radio, the default setting for this function of the new radio type is restored.

The following matrix shows the **a-mpdu enable** command and router compatibility:

Model	Description
MSR800	Available for MSR800-W and MSR800-10-W
MSR 900	No
MSR900-E	Available for MSR900-E-W
MSR 930	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT
MSR 20-1X	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 20	Only available for routers with a SIC-WLAN module that supports 802.11n

Model	Description
MSR 30	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 50	Only available for routers with a SIC-WLAN module that supports 802.11n

Examples

Disable the A-MPDU function of the current WLAN radio interface.

```
<sysname> system-view
[sysname] interface WLAN-Radio 2/0
[sysname-WLAN-Radio2/0] undo a-mpdu enable
```

a-msdu enable

Use **a-msdu enable** to enable the A-MSDU function for a radio.

Use **undo a-msdu enable** to disable the A-MSDU function for a radio.

Syntax

a-msdu enable

undo a-msdu enable

Default

The A-MSDU function is enabled.

Views

WLAN-radio interface view

Default command level

2: System level

Usage guidelines

This command is only effective on 802.11n radios. If you change the radio type of an 802.11n radio, the default setting for this function of the new radio type is restored.

The device only receives but does not send A-MSDU frames.

The following matrix shows the **a-msdu enable** command and router compatibility:

Model	Description
MSR800	Available for MSR800-W and MSR800-10-W
MSR 900	No
MSR900-E	Available for MSR900-E-W
MSR 930	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT
MSR 20-1X	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 20	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 30	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 50	Only available for routers with a SIC-WLAN module that supports 802.11n

Examples

Disable the A-MSDU function of the current WLAN radio interface.

```
<sysname> system-view
```

```
[sysname] interface WLAN-Radio 2/0
[sysname-WLAN-Radio2/0] undo a-msdu enable
```

antenna type

Use **antenna type** to specify the antenna type.

Use **undo antenna type** to restore the default.

Syntax

antenna type *type*

undo antenna type

Default

The default setting for the command depends on the device model.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

type: Specifies the antenna type.

Examples

Specify the antenna type.

```
<sysname> system-view
[sysname] interface wlan-radio 2/0
[sysname-WLAN-Radio2/0] antenna type 3CWE596
```

beacon ssid-hide

Use **beacon ssid-hide** to disable the advertising of the Service Set Identifier (SSID) in beacon frames.

Use **undo beacon ssid-hide** to restore the default.

Syntax

beacon ssid-hide

undo beacon ssid-hide

Default

The SSID is advertised in beacon frames.

Views

Service template view

Default command level

2: System level

Usage guidelines

If the advertising of the SSID in beacon frames is disabled, the SSID must be configured for the clients to associate with the AP.

Disabling the advertising of the SSID in beacon frames inhibits wireless security. Allowing the advertising of the SSID in beacon frames enables clients to discover an AP more easily.

Examples

Disable the advertising of the SSID in beacon frames.

```
<Sysname> system-view
[Sysname] wlan service-template 1 clear
[Sysname-wlan-st-1] beacon ssid-hide
```

beacon-interval

Use **beacon-interval** to set the interval for sending beacon frames. Beacon frames are transmitted at a regular interval to allow mobile clients to join the network.

Use **undo beacon-interval** to restore the default beacon interval.

Syntax

beacon-interval *interval*

undo beacon-interval

Default

The beacon interval is 100 TUs.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

interval: Specifies the interval for sending beacon frames. The value is in the range of 32 to 8191 time units (TUs).

Examples

Specify the beacon interval as 1000 TUs.

```
<Sysname> System-view
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] beacon-interval 1000
```

channel

Use **channel** to specify a channel for the radio.

Use **undo channel** to restore the default.

Syntax

channel { *channel-number* | **auto** }

undo channel

Default

auto mode is set.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

channel-number: Specifies a channel. The working channels depend on the country code and radio mode. The channel list depends on your device model.

auto: Specifies that the channel is automatically selected by the device according to the actual environment during system initialization.

Usage guidelines

Different radios support different channels. Channels may differ for each country.

Examples

Specify channel 6 for radio interface 1/0/2.

```
<Sysname> system-view
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] radio-type dot11b
[Sysname-WLAN-Radio2/0] channel 6
```

channel band-width

Use **channel band-width** to specify the channel bandwidth of the 802.11n radio.

Use **undo channel band-width** to restore the default.

Syntax

channel band-width { **20** | **40** }

undo channel band-width

Default

The channel bandwidth of the 802.11gn radio is 20 MHz.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

20: Specifies the channel bandwidth of the 802.11n radio as 20 MHz.

40: Specifies the channel bandwidth of the 802.11n radio as 40 MHz.

Usage guidelines

This command is only effective on 802.11n radios.

If you change the radio type of an 802.11n radio, the default setting for this function of the new radio type is restored.

If the channel bandwidth of the radio is set to 40 MHz, a 40 MHz channel is used as the working channel. If no 40 MHz channel is available, only a 20 MHz channel can be used. For more information, see *IEEE 802.11n-2009*.

The following matrix shows the **channel band-width** command and router compatibility:

Model	Description
MSR800	Available for MSR800-W and MSR800-10-W
MSR 900	No
MSR900-E	Available for MSR900-E-W
MSR 930	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT
MSR 20-1X	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 20	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 30	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 50	Only available for routers with a SIC-WLAN module that supports 802.11n

Examples

Configure the channel bandwidth of the radio as 20 MHz.

```
<sysname> system-view
[sysname] interface Wlan-radio 2/0
[sysname-WLAN-Radio2/0] radio-type dot11gn
[sysname-WLAN-Radio2/0] channel band-width 20
```

client dot11n-only

Use **client dot11n-only** to only allow 802.11n client access.

Use **undo client dot11n-only** to restore the default.

Syntax

client dot11n-only

undo client dot11n-only

Default

An 802.11gn radio permits both 802.11b/g and 802.11gn client access.

Views

WLAN radio interface view

Default command level

2: System level

Usage guidelines

The **client dot11n-only** command prohibits non-802.11n clients from access. To provide access for all 802.11b/g clients, disable this command.

The following matrix shows the **client dot11n-only** command and router compatibility:

Model	Description
MSR800	Available for MSR800-W and MSR800-10-W
MSR 900	No
MSR900-E	Available for MSR900-E-W
MSR 930	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT
MSR 20-1X	Only available for routers with a SIC-WLAN module that supports 802.11n

Model	Description
MSR 20	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 30	Only available for routers with a SIC-WLAN module that supports 802.11n
MSR 50	Only available for routers with a SIC-WLAN module that supports 802.11n

Examples

Configure the radio to allow only 802.11n clients to access.

```
<sysname> system-view
[sysname] interface Wlan-radio 2/0
[sysname-WLAN-Radio2/0] radio-type dot11gn
[sysname-WLAN-Radio2/0] client dot11n-only
```

client max-count (service template view)

Use **client max-count** to specify the maximum number of allowed clients for the radio policy.

Use **undo client max-count** to restore the default.

Syntax

client max-count *max-number*

undo client max-count

Default

Up to 32 clients can be associated with an SSID on a radio.

Views

Service template view

Default command level

2: System level

Parameters

max-number: Maximum number of clients associated with an SSID, in the range of 1 to 64.

Usage guidelines

When the maximum number is reached, the SSID is automatically hidden.

Examples

Specify the maximum number of clients associated with the SSID **service** on a radio as 10.

```
<Sysname> system-view
[Sysname] wlan service-template 1 clear
[Sysname-wlan-st-1] ssid service
[Sysname-wlan-st-1] client max-count 10
```

display wlan client

Use **display wlan client** to display WLAN client information. The information is displayed in the order of client MAC address.

Syntax

display wlan client { **interface wlan-radio** [*radio-number*] | **mac-address** *mac-address* | **service-template** *service-template-number* } [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

interface wlan-radio *radio-number*: Displays information about clients that are attached to the specified WLAN radio interface.

mac-address *mac-address*: Specifies the MAC address of a client.

service-template *service-template-number*: Displays client information based on the specified service template. The service template number is in the range of 1 to 1024.

verbose: Displays detailed client information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Examples

Display information about all the clients.

```
<Sysname> display wlan client
Total Number of Clients           : 3
                              Client Information
 SSID: office
------------------------------------------------------------------------------
 MAC Address   User Name            APID/RID IP Address              VLAN
------------------------------------------------------------------------------
000f-e265-6400 –NA-                  1/1     1.1.1.1                 1
000f-e265-6401 user                 1024/1   3.0.0.3                 3
000f-e265-6402 mac@office.com       103 /1   FE:11:12:03::11:25:13   1
```

Table 4 Command output

Field	Description
SSID	SSID with which the client is associated.
MAC address	MAC address of the client.
User Name	Username of the client: • The field is displayed as -NA- if the client adopts plain-text authentication or cipher-text authentication with no username. • The field is irrelevant to the portal authentication method. If the client uses the portal authentication method, the field does not display the portal username of the client.

Field	Description
APID/RID	ID of the AP or radio that the client is associated with.
IP Address	IP address of the client.
VLAN	VLAN to which the client belongs.

Display detailed information about all clients.

```
<Sysname> display wlan client verbose
 Total Number of Clients           : 1
                              Client Information
--------------------------------------------------------------------------
  MAC Address                      : 0014-6c91-9a14
  User Name                        : Guest
  AID                              : 251
  Radio Interface                  : WLAN-Radio2/0
  SSID                             : nsw-nsw
  BSSID                            : 000f-e2cc-2022
  Port                             : WLAN-BSS1
  VLAN                             : 1
  State                            : Running
  Power Save Mode                  : Sleep
  Wireless Mode                    : 11gn
Channel Band-width                : 20MHz
  SM Power Save Enable             : Disabled
  Short GI for 20MHz               : Not Supported
  Short GI for 40MHz               : Not Supported
  Support MCS Set                  : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
  BLOCK ACK-TID 0                  : BOTH
  QoS Mode                         : WMM
  Listen Interval (Beacon Interval) : 10
  RSSI                             : 25
  Rx/Tx Rate                       : 48/54
  Client Type                      : RSN
  Authentication Method            : Open System
  AKM Method                       : Dot1X
  4-Way Handshake State            : PTKINITDONE
  Group Key State                  : IDLE
  Encryption Cipher                : CCMP
  Roam Status                      : Normal
 Roam Count                       : 0
  Up Time (hh:mm:ss)               : 00:05:15
--------------------------------------------------------------------------------
```

Table 5 Command output

Field	Description
MAC address	MAC address of the client.
User Name	Username of the client: • The field is displayed as -NA- if the client adopts plain-text authentication or

Field	Description
	cipher-text authentication with no username. • The field is irrelevant to the portal authentication method. If the client uses the portal authentication method, the field does not display the portal username of the client.
AID	Association ID of the client.
Radio Interface	WLAN radio interface.
SSID	SSID of the client.
BSSID	ID of the BSS.
Port	WLAN-DBSS interface associated with the client.
VLAN	VLAN to which the client belongs.
State	State of the client such as running.
Power Save Mode	Client's power save mode such as active or sleep.
Wireless Mode	Wireless mode such as 802.11b, 802.11g, 802.11gn. **IMPORTANT:** Support for the wireless mode depends on the device model.
Channel Band-width	Channel bandwidth, 20 MHz or 40 MHz.
SM Power Save Enable	SM Power Save enables a client to have one antenna in the active state, and others in sleep state to save power. • **Enabled**—SM Power Save is enabled. • **Disabled**—SM Power Save is disabled.
Short GI for 20MHz	Whether the client supports short GI when its channel bandwidth is 20 MHz.
Short GI for 40MHz	Whether the client supports short GI when its channel bandwidth is 40 MHz.
Support MCS Set	MCS supported by the client.
BLOCK ACK-TID 0	BLOCK ACK is negotiated based on traffic identifier (TID) 0: • **OUT**—Outbound direction. • **IN**—Inbound direction. • **BOTH**—Both outbound and inbound directions.
QoS Mode	WMM indicates that the WMM function is supported; None indicates that the WMM function is not supported. WMM information negotiation is carried out between an AP and a client that both support WMM.
Listen Interval(Beacon Interval)	Number of times the client has woken up to listen to beacon frames.
RSSI	Received signal strength indication. This value indicates the client signal strength detected by the AP.
Rx/Tx Rate	Represents the receiving and sending rates of the frames such as data, management, and control frames.
Client Type	Client type such as RSN, WPA, or Pre-RSN.
Authentication Method	Authentication method such as open system or shared key.
AKM Method	AKM suite used such as Dot1X or PSK.
4-Way Handshake State	Display either of the 4-way handshake states: • **IDLE**—Displayed in initial state. • **PTKSTART**—Displayed when the 4–way handshake is initialized.

Field	Description
	• **PTKNEGOTIATING**—Displayed after sending valid message 3. • **PTKINITDONE**—Displayed when the 4-way handshake is successful.
Group Key State	Display the group key state such as: • **IDLE**—Displayed in initial state. • **REKEYNEGOTIATE**—Displayed after the AC sends the initial message to the client. • **REKEYESTABLISHED**—Displayed when re-keying is successful.
Encryption Cipher	Encryption cipher such as clear or crypto.
Roam Status	Display the roam status such as Normal or Fast Roaming.
Roam Count	Roaming count of the client, including intra-AC roaming and inter-AC roaming.
Up Time	Time for which the client has been associated with the AP.

display wlan service-template

Use **display wlan service-template** to display WLAN service template information. If no service template is specified, all service templates are displayed.

Syntax

display wlan service-template [*service-template-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

service-template-number: Number of a service template, in the range of 1 to 1024.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the configuration information for service template 1.

```
<Sysname> display wlan service-template 1
                          Service Template Parameters
--------------------------------------------------------------------------------
 Service Template Number      : 1
 SSID                         : nsw-nsw
 Service Template Type        : Crypto
 Security IE                  : RSN WPA
 Authentication Method        : Open System
 SSID-hide                    : Disabled
```

```
 Cipher Suite                 : TKIP CCMP
 WEP Key Index  1             : WEP40
 WEP Key Mode                 : ASCII
 WEP Key                      : -_'PV5%9O`CQ=^Q`MAF4<1!!
 TKIP Countermeasure Time(s)  : 60
 PTK Life Time(s)             : 180
 GTK Rekey                    : Enabled
 GTK Rekey Method             : Packet-based
 GTK Rekey Packets            : 5000
 Service Template Status      : Enabled
 Maximum clients per BSS      : 35
------------------------------------------------------------------------------
```

Table 6 Command output

Field	Description
Service Template Number	Current service template number.
SSID	SSID that is associated with the client.
Service Template Type	Service template type **crypto** or **clear**.
Security IE	Security IE such as WPA and WPA2 (RSN).
Authentication Method	Authentication used, open system or shared key.
SSID-hide	Enabled or disabled.
Cipher Suite	Cipher suite such as AES-CCMP, TKIP, WEP40, WEP104 or WEP128.
WEP Key Index	Key index to encrypt or decrypt frames.
WEP Key Mode	WEP key format: • **HEX**—Hexadecimal string. • **ASCII**—ASCII character string.
TKIP Countermeasure Time(s)	Counter measure time for MIC failure in seconds.
PTK Life Time(s)	PTK lifetime in seconds.
GTK Rekey	GTK rekey configured.
GTK Rekey Method	GTK rekey method configured such as packet based or time based.
GTK Rekey Packets	Number of packets for GTK rekey.
Service Template Status	Status such as enabled or disabled.
Maximum clients per BSS	Maximum number of associated clients per BSS.

display wlan statistics client

Use **display wlan statistics client** to display client statistics.

Syntax

display wlan statistics client { **all** | **mac-address** *mac-address* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

client: Displays client statistics.

all: Displays the statistics of all clients.

mac-address *mac-address*: Displays the statistics of the client with the specified MAC address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the statistics of all the clients.

```
<Sysname> display wlan statistics client all
                                Client Statistics
--------------------------------------------------------------------------------
 AP Name                          : ap1
 Radio Id                         : 1
 SSID                             : office
 BSSID                            : 000f-e2ff-7700
 MAC Address                      : 0014-6c8a-43ff
 RSSI                             : 31
--------------------------------------------------------------------------------
 Transmitted Frames:
 Back Ground (Frames/Bytes)       : 0/0
 Best Effort (Frames/Bytes)       : 9/1230
 Video (Frames/Bytes)             : 0/0
 Voice (Frames/Bytes)             : 2/76
 Received Frames:
 Back Ground (Frames/Bytes)       : 0/0
 Best Effort (Frames/Bytes)       : 18/2437
 Video (Frames/Bytes)             : 0/0
 Voice (Frames/Bytes)             : 7/468
 Discarded Frames:
 Back Ground (Frames/Bytes)       : 0/0
 Best Effort (Frames/Bytes)       : 0/0
 Video (Frames/Bytes)             : 0/0
 Voice (Frames/Bytes)             : 5/389
--------------------------------------------------------------------------------
```

Table 7 Command output

Field	Description
SSID	SSID to which the client is associated.
BSSID	ID of the BSS.

Field	Description
MAC Address	MAC address of the client.
RSSI	Received Signal Strength Indicator. It indicates the client signal strength detected by the AP.
Transmitted Frames	Transmitted Frames.
Back Ground(Frames/Bytes)	Statistics of background traffic.
Best Effort(Frames/Bytes)	Statistics of best effort traffic.
Video(Frames/Bytes)	Statistics of video traffic.
Voice(Frames/Bytes)	Statistics of voice traffic.
Received Frames	Received frames.
Discarded Frames	Discarded frames.

Statistics for background, best effort, video, and voice traffic are only for QoS-capable clients. For QoS-incapable clients, only best effort traffic statistics are available (including SVP packets) and might be inconsistent with the real physical output queues because the priority-queue statistics can only identify priorities carried in Dot11E and WMM packets. Otherwise, statistics of received packets cannot be collected.

display wlan statistics service-template

Use **display wlan statistics service-template** to display service template statistics.

Use **display wlan statistics service-template** *service-template-number* **connect-history** to display the connection statistics for all APs bound to the service template.

Syntax

display wlan statistics service-template *service-template-number* [**connect-history**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

service-template-number: Service template number in the range of 1 to 1024.

connection-history: Displays the connection history.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the statistics of service template 1.

```
<Sysname> display wlan statistics service-template 1
                        Service Template Statistics
```

```
--------------------------------------------------------------------------------
Service Template           : 1
--------------------------------------------------------------------------------
AP Name                    : ap1
 Radio                     : 1
 Receive                   :
    Frame Count            : 1713
    Frame Bytes            : 487061
    Data Frame Count       : 1683
    Data Frame Bytes       : 485761
    Associate Frame Count  : 2
 Send                      :
    Frame Count            : 62113
    Frame Bytes            : 25142076
    Data Frame Count       : 55978
    Data Frame Bytes       : 22626600
    Associate Frame Count  : 2
--------------------------------------------------------------------------------
```

Table 8 Command output

Field	Description
Service Template	Service template number.
AP Name	AP name.
Receive	Receive statistics: • **Frame Count**—Number of frames received. • **Frame Bytes**—Number of bytes received. • **Data Frame Count**—Number of data frames received. • **Data Frame Bytes**—Number of data bytes received. • **Associate Frame Count**—Number of association requests received.
Send	Send statistics: • **Frame Count**—Number of frames sent. • **Frame Bytes**—Number of bytes sent. • **Data Frame Count**—Number of data frames sent. • **Data Frame Bytes**—Number of data bytes sent. • **Associate Frame Count**—Number of association requests sent.

Display the connection history of service template 1.

```
<Sysname> display wlan statistics service-template 1 connect-history
                           Connect History
--------------------------------------------------------------------------------
 Service Template          : office
--------------------------------------------------------------------------------
 AP Name                   : ap1
 Radio                     : 1
 Associations              : 132
 Failures                  : 3
 Reassociations            : 30
```

```
 Rejections                 : 12
 Exceptional Deassociations : 2
 Current Associations       : 57
------------------------------------------------------------------------------
 AP Name                    : ap1
 Radio                      : 2
 Associations               : 1004
 Failures                   : 35
 Reassociations             : 59
 Rejections                 : 4
 Exceptional Deassociations : 22
 Current Associations       : 300
------------------------------------------------------------------------------
```

Table 9 Command output

Field	Description
Service Template	Service template number.
AP name	AP name.
Radio	Radio number.
Associations	Total number of associations.
Failures	Total number of failed associations.
Reassociations	Total number of reassociations.
Rejections	Total number of associations rejected.
Exceptional Deassociations	Total number of exceptional associations.
Current Associations	Number of current associations.

distance

Use **distance** to configure the maximum distance that the radio can cover.

Use **undo distance** to restore the default.

Syntax

distance *distance*

undo distance

Default

The radio can cover 1 km (0.62 miles) at most.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

distance: Specifies the maximum distance that the radio can cover, in the range of 1 to 40 km (0.62 to 24.86 miles).

Examples

Configure the maximum distance that the radio can cover as 5 km (3.11 miles).

```
<Sysname> system-view
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] distance 5
```

dtim

Use **dtim** to set the number of beacon intervals an AP waits before it sends buffered multicast and broadcast frames. The AP sends buffered broadcast/multicast frames when the DTIM counter reaches the configured value.

Use **undo dtim** to restore the default.

Syntax

dtim *counter*

undo dtim

Default

The DTIM is 1.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

counter: Number of beacon intervals between DTIM transmissions. The value is in the range of 1 to 31.

Examples

Set the DTIM counter to 10.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] dtim 10
```

fast-association enable

Use **fast-association enable** to enable fast association.

Use **undo fast-association enable** to disable fast association.

Syntax

fast-association enable

undo fast-association enable

Default

Fast association is disabled.

Views

Service template view

Default command level

2: System level

Usage guidelines

When fast association is enabled, the AP does not perform band navigation and load balancing calculations for clients bound to the SSID.

Examples

Enable fast association.

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] fast-association enable
```

fragment-threshold

Use **fragment-threshold** to specify the maximum length of frames that can be transmitted without fragmentation. A packet that exceeds the specified fragment threshold is fragmented.

Use **undo fragment-threshold** to restore the default value.

Syntax

fragment-threshold *size*

undo fragment-threshold

Default

The fragment threshold is 2346 bytes. Frames that exceed 2346 bytes are fragmented.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

size: Maximum frame length without fragmentation. The value is in the range of 256 to 2346 bytes and must be an even number.

Examples

Specify the fragment threshold as 2048 bytes.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] fragment-threshold 2048
```

long-retry threshold

Use **long-retry threshold** to set the number of re-transmission attempts for frames larger than the RTS threshold.

Use **undo long-retry threshold** to restore the default.

Syntax

long-retry threshold *count*

undo long-retry threshold

Default

The long retry threshold is 4.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

count: Number of retransmission attempts for frames larger than the RTS threshold, in the range of 1 to 15.

Examples

Specify the long-retry threshold as 10.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] long-retry threshold 10
```

max-power

Use **max-power** to configure the maximum transmission power on the radio.

Use **undo max-power** to restore the default.

Syntax

max-power *radio-power*

undo max-power

Default

The maximum radio power varies with country codes, channels, AP models, radio types, and antenna types. If 802.11n is adopted, the maximum radio power also depends on the bandwidth mode.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

radio-power: Maximum radio transmission power, which varies with country codes and radio types.

Examples

Specify the max transmission power of radio 2/0 as 5.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] radio-type dot11b
[Sysname-WLAN-Radio2/0] max-power 5
```

max-rx-duration

Use **max-rx-duration** to specify the interval for the AP to hold a received frame. An AP holds received packets in its buffer memory.

Use **undo max-rx-duration** to restore the default.

Syntax

max-rx-duration *interval*

undo max-rx-duration

Default

The max-rx-duration is 2000 milliseconds.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

interval: Interval for which a frame received by an AP can stay in the buffer memory. The value is in the range of 500 to 250000 milliseconds.

Examples

Set the max-rx-duration as 5000 milliseconds.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] max-rx-duration 5000
```

preamble

Use **preamble** to specify the type of preamble an AP can support.

Syntax

preamble { **long** | **short** }

undo preamble

Default

The short preamble is supported.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

long: Indicates that only frames with a long preamble can be transmitted.

short: Indicates that frames with either a short preamble or a long preamble can be transmitted.

Usage guidelines

Preamble is a pattern of bits at the beginning of a frame so that the receiver can sync up and be ready for the real data. There are two different kinds of preambles, short and long.

802.11a and 802.11an do not support this configuration.

Examples

Configure the AP to support long preamble.

```
<Sysname> system-view
```

```
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] radio-type dot11b
[Sysname-WLAN-Radio2/0] preamble long
```

protection-mode

Use **protection-mode** to specify a collision avoidance mechanism.

Use **undo protection-mode** to restore the default.

Syntax

protection-mode { **cts-to-self** | **rts-cts** }

undo protection-mode

Default

The collision avoidance mechanism is CTS-to-Self.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

cts-to-self: Specifies the Clear to Send (CTS)-to-Self collision avoidance mechanism.

rts-cts: Specifies the Request to Send (RTS)/CTS collision avoidance mechanism.

Usage guidelines

Compared with RTS/CTS, CTS-to-Self reduces the number of control frames. However, data collisions still occur when some clients are hidden and thus cannot receive the CTS frames sent by the AP. Therefore, the RTS/CTS mechanism can solve the data collision problem in a larger coverage than RTS/CTS.

For more information about CTS-to-Self and RTS/CTS, see *WLAN Configuration Guide*.

Examples

Configure the collision avoidance mechanism as RTS/CTS.

```
<Sysname> system-view
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] protection-mode rts-cts
```

radio-type

Use **radio-type** to specify the radio type to be used by a radio.

Use **undo radio-type** to restore the default.

Syntax

radio-type { **dot11b** | **dot11g** | **dot11gn** }

undo radio-type

Default

The default radio type depends on the device model.

Views

WLAN radio interface view

Parameters

dot 11b: Specifies the 802.11b radio type.

dot 11g: Specifies the 802.11g radio type.

dot11gn: Specifies the 802.11g/n (2.4 GHz) radio type.

Usage guidelines

The default radio type depends on the device model. WLAN allows you to modify the default radio type for different types of AP.

The following matrix shows the **dot11b**, **dot11g**, and **dot11gn** keywords and router compatibility:

Model	Description
MSR800	The **dot11gn** keyword is available only for MSR800-W and MSR800-10-W.
MSR 900	The **dot11gn** keyword is not supported.
MSR900-E	The **dot11gn** keyword is only available for MSR900-E-W.
MSR 930	The **dot11gn** keyword is only available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT.
MSR 20-1X	The **dot11gn** keyword is only available for routers with a SIC-WLAN module that supports 802.11n
MSR 20	The **dot11gn** keyword is only available for routers with a SIC-WLAN module that supports 802.11n
MSR 30	The **dot11gn** keyword is only available for routers with a SIC-WLAN module that supports 802.11n
MSR 50	The **dot11gn** keyword is only available for routers with a SIC-WLAN module that supports 802.11n

Examples

Specify the radio type as 802.11g for interface WLAN-Radio 2/0.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] radio-type dot11g
```

reset wlan client

Use **reset wlan client** to cut off a client or all clients. When this command is used, the AP sends a de-authentication frame to the client and the client is removed from the WLAN service.

Syntax

reset wlan client { **all** | **mac-address** *mac-address* }

Views

User view

Default command level

2: System level

Parameters

all: Cuts off all clients.

mac address *mac-address*: Cuts off the client specified by the MAC address.

Examples

Cut off the client with MAC address 000f-e2cc-8501.

```
<Sysname> reset wlan client mac-address 000f-e2cc-8501
```

reset wlan statistics

Use **reset wlan statistics** to clear client or radio statistics.

Syntax

reset wlan statistics client { **all** | **mac-address** *mac-address* }

Views

User view

Default command level

2: System level

Parameters

all: Clears the statistics of all clients.

mac-address *mac-address*: Clears the statistics of the client.

Examples

Clear the statistics of all clients.

```
<Sysname> reset wlan statistics client all
```

rts-threshold

Use **rts-threshold** to specify the request to send (RTS) threshold length. If a frame is larger than this value, the RTS mechanism is used.

Use **undo rts-threshold** to restore the default.

Syntax

rts-threshold *size*

undo rts-threshold

Default

The RTS threshold is 2346 bytes.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

size: Length of frames for which the request to send (RTS) method is used. The value is in the range of 0 to 2346 bytes.

Usage guidelines

Request to Send (RTS) is used to avoid data sending collisions in a WLAN. You need to set a rational value:

A small value causes RTS packets to be sent more often, consuming more of the available bandwidth. However, the system can recover more quickly from interference or collisions when RTS packets are sent more frequently.

Examples

Specify the RTS threshold as 2046 bytes.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] rts-threshold 2046
```

service-template (WLAN radio interface view)

Use **service-template** to map a service template to the current radio.

Syntax

service-template *service-template-number* **interface wlan-bss** *wlan-bss-number*

undo service-template *service-template-number*

Default

No service-template is mapped to a WLAN-BSS interface on a WLAN radio interface.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

service-template-number: Number of a service template, in the range of 1 to 1024.

wlan-bss-number: Number of a WLAN-BSS interface in, the range of 0 to 1023.

Examples

Map service template 1 to interface WLAN-BSS 1 on interface WLAN-Radio 2/0.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] service-template 1 interface WLAN-BSS 1
```

service-template (service template view)

Use **service-template** to map a service template to a WLAN-BSS interface on the current WLAN radio interface.

Use **undo service-template** to remove the mapping.

Syntax

service-template { **disable** | **enable** }

Default

The service template is disabled.

Views

Service template view

Default command level

2: System level

Parameters

disable: Disables the service template.

enable: Enables the service template.

Examples

Enable service template 1.

```
<Sysname> system-view
[Sysname] wlan service-template 1 clear
[Sysname-wlan-st-1] ssid clear
[Sysname-wlan-st-1] authentication-method open-system
[Sysname-wlan-st-1] service-template enable
```

short-gi enable

Use **short-gi enable** to enable the short GI function.

Use **undo short-gi enable** to disable the short GI function.

Syntax

short-gi enable

undo short-gi enable

Default

The short GI function is enabled.

Views

WLAN radio interface view

Default command level

2: System level

Usage guidelines

This command is only effective on 802.11n radios.

If you change the radio type of an 802.11n radio, the default setting for this function of the new radio type is restored.

Delays might occur during receiving radio signals due to factors like multi-path reception. Therefore, a subsequently sent frame might interfere with a previously sent frame. The GI function is used to avoid such interference.

The GI interval in 802.11a/g is 800 us. The short GI function can be configured for 802.11n. This can shorten the GI interval to 400 ns, which increases the data speed by 10 percent.

Examples

Disable the short GI function.

```
<sysname> system-view
[sysname] interface WLAN-Radio2/0
[sysname-WLAN-Radio2/0] undo short-gi enable
```

short-retry threshold

Use **short-retry threshold** to specify the maximum number of attempts to transmit a frame less than the RTS threshold.

Use **undo short-retry threshold** to restore the default.

Syntax

short-retry threshold *count*

undo short-retry threshold

Default

The short retry threshold is 7.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

count: Number of times the AP can send a short unicast frame (less than the RTS threshold) if no acknowledgment is received for it. The value is in the range of 1 to 15.

Examples

Specify the short retry threshold as 10.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio 2/0
[Sysname-WLAN-Radio2/0] short-retry threshold 10
```

ssid

Use **ssid** to set the SSID for the current service template.

Use **undo ssid** to remove the SSID.

Syntax

ssid *ssid-name*

undo ssid

Default

No SSID is set for the service template.

Views

Service template view

Default command level

2: System level

Parameters

ssid-name: Name of the service set identifier, a case-sensitive string of 1 to 32 characters.

Usage guidelines

An SSID should be as unique as possible. For security, do not include the company name in the SSID. Additionally, do not use a long random string as the SSID. Doing so only adds payload to the header field and does not improve wireless security.

Examples

Set the SSID as **firstfloor** for service template 1.

```
<Sysname> system-view
[Sysname] wlan service-template 1 clear
[Sysname-wlan-st-1] ssid firstfloor
```

wlan broadcast-probe reply

Use **wlan broadcast-probe reply** to enable the AP to respond to the probe requests without SSID.

Use **undo wlan broadcast-probe reply** to remove the configuration to cause the AP to only respond to probe requests that carry the specified SSID.

Syntax

wlan broadcast-probe reply

undo wlan broadcast-probe reply

Default

An AP responds to probe requests without SSID.

Views

System view

Examples

Enable the AP to respond to probe requests without SSID.

```
<Sysname> system-view
[Sysname] wlan broadcast-probe reply
```

wlan client idle-timeout

Use **wlan client idle-timeout** to specify the client idle timeout.

Use **undo wlan client idle-timeout** to restore the default.

Syntax

wlan client idle-timeout *interval*

undo wlan client idle-timeout

Default

The client idle timeout is 3600 seconds.

Views

System view

Default command level

2: System level

Parameters

interval: Maximum interval for which the link between the AP and a client (power-save or awake) can be idle. The value is in the range of 60 to 86400 seconds.

Usage guidelines

If the AP does not receive any data from a client within the client idle timeout interval, it removes the client from the network.

Examples

Specify the client idle timeout as 600 seconds.

```
<Sysname> system-view
[Sysname] wlan client idle-timeout 600
```

wlan client keep-alive

Use **client keep-alive** to specify the client keep alive interval.

Use **undo client keep-alive** to restore the default.

Syntax

wlan client keep-alive *interval*

undo wlan client keep-alive

Default

The client keep-alive functionality is disabled.

Views

System view

Default command level

2: System level

Parameters

interval: Interval between keep alive requests. The value is in the range of 3 to 1800 seconds.

Usage guidelines

The keep-alive mechanism is used to detect clients that are segregated from the system for various reasons such as power failure or crash, and disconnect them from the AP.

Examples

Specify the client keep-alive interval as 60 seconds.

```
<Sysname> system-view
[Sysname] wlan client keep-alive 60
```

wlan country-code

Use **wlan country-code** to specify the global country code.

Use **undo wlan country-code** to restore the default.

Syntax

wlan country-code *code*

undo wlan country-code

Default

The country code for North American models is US, and for other models is CN.

Views

System view

Default command level

2: System level

Parameters

code: Specifies a global country code. See Table 10.

Table 10 Country code information

Country	Code	Country	Code
Andorra	AD	Korea, Republic of Korea	KR
United Arab Emirates	AE	Kenya	KE
Albania	AL	Kuwait	KW
Armenia	AM	Kazakhstan	KZ
Australia	AU	Lebanon	LB
Argentina	AR	Liechtenstein	LI
Australia	AT	Sri Lanka	LK
Azerbaijan	AZ	Lithuania	LT
Bosnia and Herzegovina	BA	Luxembourg	LU
Belgium	BE	Latvia	LV
Bulgaria	BG	Libyan	LY
Bahrain	BH	Morocco	MA
Brunei Darussalam	BN	Monaco	MC
Bolivia	BO	Moldova	MD
Brazil	BR	Macedonia	MK
Bahamas	BS	Macau	MO
Belarus	BY	Martinique	MQ
Belize	BZ	Malta	MT
Canada	CA	Mauritius	MU
Switzerland	CH	Mexico	MX
Cote d'ivoire	CI	Malay Archipelago	MY
Chile	CL	Namibia	NA
China	CN	Nigeria	NG
Colombia	CO	Nicaragua	NI
Costarica	CR	Netherlands	NL
Serbia	RS	Norway	NO
Cyprus	CY	New Zealand	NZ
Czech Republic	CZ	Oman	OM
Germany	DE	Panama	PA
Denmark	DK	Peru	PE
Dominica	DO	Poland	PL
Algeria	DZ	Philippines	PH

Country	Code	Country	Code
Ecuador	EC	Pakistan	PK
Estonia	EE	Puerto Rico	PR
Egypt	EG	Portugal	PT
Spain	ES	Paraguay	PY
Faroe Islands	FO	Qatar	QA
Finland	FI	Romania	RO
France	FR	Russian Federation	RU
Britain	GB	Saudi Arabia	SA
Georgia	GE	Sweden	SE
Gibraltar	GI	Singapore	SG
Greenland	GL	Slovenia	SI
Guadeloupe	GP	Slovak	SK
Greece	GR	San Marino	SM
Guatemala	GT	Salvador	SV
Guyana	GY	Syrian	SY
Honduras	HN	Thailand	TH
Hong Kong	HK	Tunisia	TN
Croatia	HR	Turkey	TR
Hungary	HU	Trinidad and Tobago	TT
Iceland	IS	Taiwan, Province of China	TW
India	IN	Ukraine	UA
Indonesia	ID	United States of America	US
Ireland	IE	Uruguay	UY
Israel	IL	Uzbekistan	UZ
Iraq	IQ	The Vatican City State	VA
Italy	IT	Venezuela	VE
Iran	IR	Virgin Islands	VI
Jamaica	JM	Vietnam	VN
Jordan	JO	Yemen	YE
Japan	JP	South Africa	ZA
Democratic People's Republic of Korea	KP	Zimbabwe	ZW

Usage guidelines

The country code determines characteristics such as the power level and the total number of channels. You must set the correct country code or area code for a WLAN device (AC or AP).

If an AP is configured with a country code in AP template view or has a fixed country code, changing the global country code does not affect the country code of the AP.

The country code for North American models cannot be modified and that for other models can be modified at the CLI.

Examples

Specify the global country code as US.

```
<Sysname> system-view
[Sysname] wlan country-code us
```

wlan link-test

Use **wlan link-test** to RFPing a client.

Syntax

wlan link-test *mac-address*

Views

User view

Default command level

1: Monitor level

Parameters

mac-address: MAC address of a client. Only clients that have been associated with the AP can be RFPinged.

Examples

Perform an RFPing operation on the client with the MAC address 000f-e201-0101.

```
<Sysname> wlan link-test 000f-e201-0101
Testing link to 000f-e201-0101, press CTRL_C to break......
                                Link Status
 RTT: Round trip time
--------------------------------------------------------------------------------
 MAC Address: 000f-e201-0101
--------------------------------------------------------------------------------
 No.    Rate(Mbps)  TxCnt   RxCnt   RSSI    Retries     RTT(ms)
--------------------------------------------------------------------------------
 0      1           5       2       62      0           0
 1      2           5       5       10      0           0
 2      5.5         5       5       10      0           1
 3      6           5       5       10      0           0
 4      9           5       5       11      0           0
 5      11          5       5       11      0           0
 6      12          5       5       10      0           0
 7      18          5       5       10      0           0
 8      24          5       5       11      0           0
 9      36          5       5       11      0           0
 10     48          5       5       10      0           0
 11     54          5       5       11      0           0
```

Table 11 RFPing operation results

Field	Description
No./MCS	• The No. field is displayed for an RFPing operation to a non 802.11n client, indicating the rate index of the client. • The MCS field is displayed for an RFPing operation to an 802.11n client, indicating the MCS value of the client.
Rate(Mbps)	Rate for the radio interface to send ping packets.
TxCnt	Number of ping packets sent by the radio interface.
RxCnt	Number of ping packets received by the radio interface from the client.
RSSI	Received signal strength indicator (RSSI).
Retries	Number of retries when the radio interface failed to send ping packets.
RTT(ms)	RTT from the time the radio interface sends a ping packet to the time it receives a response from the client.

wlan service-template

Use **wlan service-template** to create a service template and enter service template view. If the service template exists, you can directly enter service template view.

Use **undo wlan service-template** to delete the service template and related configurations. If the specified service template is mapped to a radio, it cannot be directly deleted before it is un-mapped.

Syntax

wlan service-template *service-template-number* { **clear** | **crypto** }

undo wlan service-template *service-template-number*

Default

No service template is configured.

Views

System view

Default command level

2: System level

Parameters

service-template-number: Number of the service template, in the range of 1 to 1024.

clear: Sets the current service template type to **clear**, which means data will be sent in clear text after the template is mapped to an AP.

crypto: Sets the current service template type to **crypto**, which means data will be sent in cipher text after the template is mapped to an AP.

Usage guidelines

You cannot change an existing service template to another type. To do so, delete the existing service template and configure a new service template with the new type.

Examples

Create service template 1.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
```

```
[Sysname-wlan-st-1]
```

Workgroup bridge configuration commands

client-mode authentication-method

Use **client-mode authentication-method** to configure the authentication method for the workgroup bridge.

Use **undo client-mode authentication-method** to restore the default.

Syntax

client-mode authentication-method { **open-system** | **shared-key** | **wpa2-psk** }

undo client-mode authentication-method

Default

The authentication method for the workgroup bridge is open system authentication.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

open-system: Specifies the open system authentication.

shared-key: Specifies the shared-key authentication.

wpa2-psk: Specifies the WPA2-PSK authentication.

Examples

Configure the authentication method for the workgroup bridge as shared-key authentication.

```
<Sysname> system-view
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] client-mode authentication-method shared-key
```

client-mode cipher-suite

Use **client-mode cipher-suite** to select the cipher suite and pre-shared key for the workgroup bridge.

Use **undo client-mode cipher-suite** to restore the default.

Syntax

client-mode cipher-suite { **ccmp** | **tkip** | { **wep40 | wep104 | wep128** } [**key-id** *key-id*] } **key pass-phrase** [**cipher | simple**] *key*

undo client-mode cipher-suite

Default

No cipher suite and pre-shared key are configured for the workgroup bridge.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

ccmp: Enables the CCMP cipher suite.

tkip: Enables the TKIP cipher suite.

wep40: Enables the WEP-40 cipher suite.

wep104: Enables the WEP-104 cipher suite.

wep128: Enables the WEP-128 cipher suite.

key-id *key-id*: Specifies the key ID. There are four static keys in WEP. The key index can be 1, 2, 3, or 4. The key corresponding to the specified key index is used for encrypting and decrypting broadcast and multicast frames.

pass-phrase: Sets the pre-shared key in character string format.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key. This key will be saved in cipher text for security purposes.

string-key: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a non-hexadecimal string of 8 to 63 characters or a 64-character hexadecimal string. If **cipher** is specified, it must be a ciphertext string of 24 to 88 characters for the WEP-40, WEP-104, and WEP-128 cipher suites, or a ciphertext string of 24 to 117 characters for the CCMP and TKIP cipher suites. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Usage guidelines

For security purposes, all keys, including keys configured in plain text, are saved in cipher text.

Examples

Configure the cipher suite and pre-shared key for the workgroup bridge.

```
<Sysname> system-view
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] client-mode cipher-suite wep40 key simple abcas
```

client-mode connect

Use **client-mode connect** to connect the workgroup bridge to the wireless network.

Syntax

client-mode connect

Views

WLAN radio interface view

Default command level

2: System level

Examples

Connect the AP in client mode to the wireless network.

```
<Sysname> system-view
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] client-mode connect
```

client-mode disconnect

Use **client-mode disconnect** to disconnect the workgroup bridge from the wireless network.

Syntax

client-mode disconnect

Views

WLAN radio interface view

Default command level

2: System level

Examples

Disconnect the workgroup bridge from the wireless network.

```
<Sysname> system-view
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] client-mode disconnect
```

client-mode interface wlan-bss

Use **client-mode interface wlan-bs** to configure the current radio interface as a workgroup bridge and bind the radio interface to a WLAN-BSS interface.

Use **undo client-mode interface wlan-bss** to disable workgroup bridge mode for the radio interface and remove the binding between the radio interface and the WLAN-BSS interface.

Syntax

client-mode interface wlan-bss *bss-id*

undo client-mode interface wlan-bss

Default

Workgroup bridge mode is disabled.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

bss-id: WLAN-BSS interface number.

Usage guidelines

Workgroup bridge related configurations can be applied only when workgroup bridge mode is enabled. When the workgroup bridge mode is disabled, all workgroup bridge related configurations are automatically removed.

Examples

Enable workgroup bridge mode for the radio interface and bind the radio interface to WLAN-BSS 1.

```
<Sysname> system-view
[Sysname] interface wlan-bss 1
[Sysname-WLAN-BSS1] quit
[Sysname] interface wlan-radio 2/0
```

```
[Sysname-WLAN-Radio2/0] client-mode interface wlan-bss 1
```

client-mode ssid

Use **client-mode ssid** to configure the SSID for the workgroup bridge .

Use **undo client-mode ssid** to disable the SSID for the workgroup bridge.

Syntax

client-mode ssid *ssid*

undo client-mode ssid

Default

No SSID is specified for the workgroup bridge.

Views

WLAN radio interface view

Default command level

2: System level

Parameters

ssid: Associated SSID, a case-sensitive string of 1 to 32 characters.

Examples

Configure the SSID for the workgroup bridge as ChinaNet-ABC.

```
<Sysname> system-view
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] client-mode ssid ChinaNet-ABC
```

display wlan client-mode radio

Use **display wlan client-mode radio** to display the configuration and connection status for the radios in workgroup bridge mode.

Syntax

display wlan client-mode radio [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the configuration and connection status for the AP in client mode.

```
<Sysname> display wlan client-mode radio
                            WLAN Client Mode
--------------------------------------------------------------------------------
 Radio                 : 2
 Mode                  : 802.11g
 Authentication Method : WPA2-PSK
 Cipher Suite          : AES-CCMP
 Key (Simple)          : ******
 WEP Key ID            : N/A
 SSID                  : ChinaNet-ABC
 BSSID                 : 6CF0-49CD-30BB
 Status                : Connected
--------------------------------------------------------------------------------
 Received Packets
    Data               : 1324939
    Management         : 34876
 Sent Packets
    Data               : 46365
 Discarded Packets     : 38272
 Rate(Rx/Tx)           : 1 2 5.5 6 9 11 12 18 24 36 48 54
 Online Duration       : 0 days 0 hours 45 minutes 5 seconds
 --------------------------------------------------------------------------------
```

Table 12 Command output

Field	Description
Radio	Radio ID.
Mode	Radio mode.
Authentication Method	Authentication method: • Open-System. • Shared-Key. • WPA2-PSK.
Cipher Suite	Cipher suite: • WEP40. • WEP104. • WEP128. • TKIP. • AES-CCMP.
Key	Key: • **(Cipher)**—Cipher-text key is displayed in cipher text. • **(Simple)**—Cipher-text key is displayed in simple text.
WEP Key ID	WEP key ID.
Status	Association status: • Connected. • Disconnected.
Received Data Packets	Number of received data frames.

Field	Description
Received Management Packets	Number of received management frames.
Sent Data Packets	Number of data frames sent.
Discarded Packets	Number of discarded frames.
Rate(Rx/Tx)	Receive and transmit rates.
Online Duration	Online duration after the radio is connected to the wireless network.

display wlan client-mode ssid

Use **display wlan client-mode ssid** to display the wireless services and signal quality scanned by the workgroup bridge.

Syntax

display wlan client-mode ssid [*ssid*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

ssid: SSID name, a case-sensitive string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the scanned wireless services and signal quality.

```
<Sysname> display wlan client-mode ssid
                                  SSID List
--------------------------------------------------------------------------------
 SSID Name                        BSSID           Type    RSSI    Quality
--------------------------------------------------------------------------------
 ChinaNet-ABC                     1A76-2435-FD21  Clear   55      *****
 Temp                             2334-5431-BDA1  WPA2    9       *
 TC                               6CF0-AAFD-12FF  WEP     22      ***
 H3C                              F7FD-FDC1-F123  WPA     40      ****
 Lab                              4138-FAB7-8545  Clear   39      ****
 Home_12345678900000000000000000  F643-ABD4-439F  WPA2    27      ***
--------------------------------------------------------------------------------
```

Table 13 Command output

Field	Description
Type	Encryption type: • Clear. • WPA. • WPA2. • WEP.
Quality	Signal quality: • *********—Excellent. • ********—Very good. • *******—Good. • ******—Low. • *****—Very low. • No Signal.

SSID-based access control configuration commands

wlan permit-ssid

Use **wlan permit-ssid** to specify a permitted SSID for a user profile.

Use **undo wlan permit-ssid** to remove a permitted SSID or all permitted SSIDs.

Syntax

wlan permit-ssid *ssid-name*

undo wlan permit-ssid [*ssid-name*]

Default

No permitted SSID is specified for a user profile, which means that users can access the WLAN through any SSID.

Views

User profile view

Default command level

2: System level

Parameters

ssid-name: Name of a permitted SSID. It is a case-sensitive string of 1 to 32 characters that can contain letters, numbers, underlines, and spaces. The maximum number of permitted SSIDs in a user profile varies depending on the device model.

Examples

Specify permitted SSID **VIPguest** for user profile **management**.

```
<System> system-view
[System] user-profile management
[System-user-profile-management] wlan permit-ssid VIPguest
```

WLAN RRM configuration commands

The terms *AP* and *fat AP* in this document refer to MSR800, MSR 900, MSR900-E, MSR 930, and MSR 20-1X routers with IEEE 802.11b/g and MSR series routers installed with a SIC WLAN module.

WLAN is not available on the following routers:

- MSR 2600.
- MSR 30-11.
- MSR 30-11E.
- MSR 30-11F.
- MSR3600-51F.

autochannel-set avoid-dot11h

Use **autochannel-set avoid-dot11h** to configure that only the non-dot11h channels of the country code are scanned during initial channel selection.

Use **undo autochannel-set** to restore the default.

Syntax

autochannel-set avoid-dot11h

undo autochannel-set

Default

All channels of the country code are scanned.

Views

WLAN RRM view

Default command level

2: System level

Usage guidelines

Some of 802.11h channels, also called radar channels, overlap some 802.11a channels. If the device operates on an overlapping channel, its service quality might be affected. With this command enabled, the device selects a working channel from non-802.11h channels belonging to the configured country code to avoid channel collision.

Examples

Configure RRM to scan only non-dot11h channels.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] autochannel-set avoid-dot11h
```

display wlan rrm

Use **display wlan rrm** to display basic RRM configuration information.

Syntax

display wlan rrm [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display RRM configuration information.

```
<Sysname> display wlan rrm
                             RRM Configuration
------------------------------------------------------------------------------
11b Configured Rates (Mbps)
   Mandatory                  : 1, 2
   Supported                  : 5.5, 11
   Disabled                   : -NA-
 11g Configured Rates (Mbps)
   Mandatory                  : 1, 2, 5.5, 11
   Supported                  : 6, 9, 12, 18, 24, 36, 48, 54
   Disabled                   : -NA-
 11b Configuration
   max-bandwidth (kbps)       : 7000
 11g Configuration
   11g Protection             : Disabled
   11g Protection Mode        : CTS-to-Self
   max-bandwidth (kbps)       : 30000
 11n Configuration
   Mandatory Maximum MCS      : -NA-
   Supported Maximum MCS      : 76
   Multicast MCS              : -NA-
   11n Protection             : Disabled
   11n Protection Mode        : CTS-to-Self
   max-bandwidth (kbps)       : 180000
 11h Configuration
   Spectrum Management        : Disabled
   Power Constraint (dBm)     : 0
   Channel Set                : All
------------------------------------------------------------------------------
```

Table 14 Command output

Field	Description
11b Configured Rates (Mbps)	802.11b rates. The same field for 802.11g has the same meaning.
Mandatory	Rates that at least one of the APs is required to support.
Supported	Additional rates supported by the client or AP.
Disabled	Rates at which an AP does not transmit data.
11g Protection	802.11g protection: Enabled or Disabled.
11g Protection Mode	802.11g protection mode: CTS-to-Self or RTS/CTS.
11n Protection Mode	802.11n protection mode: CTS-to-Self or RTS/CTS.
11h Configuration	802.11h configuration.
Spectrum Management	Enabled or disabled.
Power Constraint (dBm)	Power constraint for all 802.11a radios. This field is not supported and displays 0.
Channel Set	All or Non-dot11h.

dot11b

Use **dot11b** to configure 802.11b rates.

Use **undo dot11b** to restore the default rates.

Syntax

dot11b { **disabled-rate** | **mandatory-rate** | **multicast-rate** | **supported-rate** } *rate-value*

undo dot11b { **disabled-rate** | **mandatory-rate** | **multicast-rate** | **supported-rate** }

Views

WLAN RRM view

Default command level

2: System level

Parameters

disabled-rate: Specifies disabled rates.

mandatory-rate: Specifies mandatory rates.

multicast-rate: Specifies multicast rates, at which the AP send multicasts to clients. Multicasts rates must be selected from the mandatory rates.

supported-rate: Specifies supported rates.

rate-value: The following rates can be specified.:

- 1 Mbps
- 2 Mbps
- 5.5 Mbps
- 11 Mbps

Examples

Configure 802.11b rates (disabled: 1; multicast: 11; supported: 11).

```
<Sysname> system-view
```

```
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11b disabled-rate 1
[Sysname-wlan-rrm] dot11b multicast-rate 11
[Sysname-wlan-rrm] dot11b supported-rate 11
```

dot11b max-bandwidth

Use **dot11b max-bandwidth** to configure the maximum 802.11b bandwidth.

Use **undo dot11b max-bandwidth** to restore the default.

Syntax

dot11b max-bandwidth *11b-bandwidth*

undo dot11b max-bandwidth

Default

The maximum 802.11b bandwidth is 7000 kbps.

Views

WLAN RRM view

Default command level

2: System level

Parameters

11b-bandwidth: Maximum 802.11b bandwidth in the range of 16 to 7000 kbps.

Examples

Configure the maximum 802.11b bandwidth as 6000 kbps.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11b max-bandwidth 6000
```

dot11g

Use **dot11g** to configure 802.11g rates.

Use **undo dot11g** to restore the default rates.

Syntax

dot11g { **disabled-rate** | **mandatory-rate** | **multicast-rate** | **supported-rate** } *rate-value*

undo dot11g { **disabled-rate** | **mandatory-rate** | **multicast-rate** | **supported-rate** }

Default

- **Disabled rate**s—None.
- **Mandatory rates**—1, 2, 5.5, and 11.
- **Multicast rates**—Automatically selected from the mandatory rates.
- **Supported rates**—6, 9, 12, 18, 24, 36, 48, and 54.

Views

WLAN RRM view

Default command level

2: System level

Parameters

disabled-rate: Specifies disabled rates.

mandatory-rate: Specifies mandatory rates.

multicast-rate: Specifies multicast rates, which are the rates at which the AP send multicasts to clients. Multicasts rates must be selected from the mandatory rates.

supported-rate: Specifies supported rates.

rate-value: The following rates can be specified.

- 1 Mbps
- 2 Mbps
- 5.5 Mbps
- 6 Mbps
- 9 Mbps
- 11 Mbps
- 12 Mbps
- 18 Mbps
- 24 Mbps
- 36 Mbps
- 48 Mbps
- 54 Mbps

Examples

Configure 802.11g rates (disabled: 2, 36; multicast: 11; supported: 54).

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11g disabled-rate 2 36
[Sysname-wlan-rrm] dot11g multicast-rate 11
[Sysname-wlan-rrm] dot11g supported-rate 54
```

dot11g max-bandwidth

Use **dot11g max-bandwidth** to configure the maximum 802.11g bandwidth.

Use **undo dot11g max-bandwidth** to restore the default.

Syntax

dot11g max-bandwidth *11g-bandwidth*

undo dot11g max-bandwidth

Default

The maximum 802.11g bandwidth 30000 kbps.

Views

WLAN RRM view

Default command level

2: System level

Parameters

11g-bandwidth: Maximum 802.11g bandwidth in kbps. It is in the range of 16 to 30000 kbps.

Examples

Configure the maximum 802.11g bandwidth as 6000 kbps.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11g max-bandwidth 6000
```

dot11g protection enable

Use **dot11g protection enable** to enable 802.11g protection.

Use **undo dot11g protection enable** to restore the default.

Syntax

dot11g protection enable

undo dot11g protection enable

Default

802.11g protection is disabled.

Views

WLAN RRM view

Default command level

2: System level

Examples

Enable 802.11g protection.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11g protection enable
```

dot11g protection-mode

Use **dot11g protection-mode** to configure the 802.11g protection mode.

Use **undo dot11g protection-mode** to restore the default.

Syntax

dot11g protection-mode { **cts-to-self** | **rts-cts** }

undo dot11g protection-mode

Default

The 802.11g protection mode is CTS-to-Self.

Views

WLAN RRM view

Default command level

2: System level

Parameters

cts-to-self: Specifies the Clear to Send (CTS)-to-Self mode.

rts-cts: Specifies the Request to Send (RTS)/CTS mode.

Examples

Configure the 802.11g protection mode as RTS/CTS.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11g protection-mode rts-cts
```

dot11n mandatory maximum-mcs

Use **dot11n mandatory maximum-mcs** to specify the maximum MCS index for 802.11n mandatory rates.

Use **undo dot11n mandatory maximum-mcs** to remove the configuration.

Syntax

dot11n mandatory maximum-mcs *index*

undo dot11n mandatory maximum-mcs

Default

No maximum MCS index is specified for 802.11n mandatory rates.

Views

RRM view

Default command level

2: System level

Parameters

index: Specifies the maximum MCS index for 802.11n mandatory rates, in the range of 0 to 76.

Usage guidelines

If you configure the **client dot11n-only** command for a radio, you must configure the maximum MCS index for 802.11n mandatory rates.

The following matrix shows the **dot11n mandatory maximum-mcs** command and router compatibility:

MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
Available for MSR800-W and MSR800-10-W	No	Available for MSR900-E-W	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n

Examples

Specify the maximum MCS index for 802.11n mandatory rates as 15.

```
<sysname> system-view
[sysname] wlan rrm
[sysname-wlan-rrm] dot11n mandatory maximum-mcs 15
```

dot11n max-bandwidth

The following matrix shows the **dot11n max-bandwidth** command and router compatibility:

MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
Available for MSR800-W and MSR800-10-W	No	Available for MSR900-E-W	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n

Use **dot11n max-bandwidth** to configure the maximum 802.11n bandwidth.

Use **undo dot11n max-bandwidth** to restore the default.

Syntax

dot11n max-bandwidth *11n-bandwidth*

undo dot11n max-bandwidth

Default

The maximum 802.11n bandwidth is 180000 kbps.

Views

WLAN RRM view

Default command level

2: System level

Parameters

11a-bandwidth: Maximum 802.11n bandwidth in the range of 16 to 180000 kbps.

Examples

Configure the maximum 802.11n bandwidth as 6000 kbps.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11n max-bandwidth 6000
```

dot11n multicast-rate

Use **dot11n multicast-rate** to specify the maximum MCS index for 802.11n multicast rates.

Use **undo dot11n multicast-rate** to remove the configuration.

Syntax

dot11n multicast-rate *index*

undo dot11n multicast-rate

Default

The maximum MCS index for 802.11n multicast rates is not configured.

Views

RRM view

Default command level

2: System level

Parameters

index: Specifies the maximum MCS index for 802.11n multicast rates, in the range of 0 to 76.

Usage guidelines

The multicast MCS is adopted only when all the clients use 802.11n.

If a non 802.11n client exists, multicast traffic is transmitted at a mandatory MCS data rate.

If you configure a multicast MCS index greater than the maximum MCS index supported by the radio, the maximum MCS index is adopted.

When the multicast MCS takes effect, the corresponding data rates defined for 20 MHz are adopted no matter whether the 802.11n radio operates in 40 MHz mode or in 20 MHz mode.

The following matrix shows the **dot11n multicast-rate** command and router compatibility:

MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
Available for MSR800-W and MSR800-10-W	No	Available for MSR900-E-W	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n

Examples

Specify the maximum MCS index for 802.11n multicast rates as 76.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11n multicast-rate 76
```

dot11n protection enable

The following matrix shows the **dot11n protection enable** command and router compatibility:

MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
Available for MSR800-W and MSR800-10-W	No	Available for MSR900-E-W	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n

Use **dot11n protection enable** to enable 802.11n protection.

Use **undo dot11n protection enable** to restore the default.

Syntax

dot11n protection enable

undo dot11n protection enable

Default

802.11n protection is disabled.

Views

WLAN RRM view

Default command level

2: System level

Examples

Enable 802.11n protection.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11n protection enable
```

dot11n protection-mode

The following matrix shows the **dot11n protection-mode** command and router compatibility:

MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
Available for MSR800-W and MSR800-10-W	No	Available for MSR900-E-W	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n

Use **dot11n protection-mode** to configure the 802.11n protection mode.

Use **undo dot11n protection-mode** to restore the default.

Syntax

dot11n protection-mode { **cts-to-self** | **rts-cts** }

undo dot11n protection-mode

Default

The 802.11n protection mode is CTS-to-Self.

Views

WLAN RRM view

Default command level

2: System level

Parameters

cts-to-self: Specifies the Clear to Send (CTS)-to-Self mode.

rts-cts: Specifies the Request to Send (RTS)/CTS mode.

Examples

Configure the 802.11n protection mode as RTS/CTS.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] dot11n protection-mode rts-cts
```

dot11n support maximum-mcs

Use **dot11n support maximum-mcs** to specify the maximum MCS index for 802.11n supported rates.

Use **undo dot11n support maximum-mcs** to restore the default.

Syntax

dot11n support maximum-mcs *index*

undo dot11n support maximum-mcs

Default

The maximum MCS index for 802.11n supported rates is 76.

Views

RRM view

Default command level

2: System level

Parameters

index: Specifies the maximum MCS index for 802.11n supported rates, in the range of 0 to 76.

Usage guidelines

The specified maximum MCS index for 802.11n supported rates must be no less than the specified maximum MCS index for 802.11n mandatory rates.

The following matrix shows the **dot11n support maximum-mcs** command and router compatibility:

MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
Available for MSR800-W and MSR800-10-W	No	Available for MSR900-E-W	Available for MSR 930-W, MSR 930-W-GU, and MSR 930-W-GT	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n	Only available for routers with a SIC-WLAN module that supports 802.11n

Examples

Specify the maximum MCS index for 802.11n supported rates as 25.

```
<sysname> system-view
[sysname] wlan rrm
[sysname-wlan-rrm] dot11n support maximum-mcs 25
```

scan report-interval

Use **scan report-interval** to set the scan report interval.

Use **undo scan report-interval** to restore the default.

Syntax

scan report-interval *seconds*

undo scan report-interval

Default

The scan report interval is 10 seconds.

Views

WLAN RRM view

Default command level

2: System level

Parameters

seconds: Interval for sending scan reports to the AC, in the range of 5 to 120 seconds.

Examples

Set the scan report interval to 20 seconds.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm] scan report-interval 20
```

scan type

Use **scan type** to set the scan type.

Use **undo scan type** to restore the default.

Syntax

scan type { **active** | **passive** }

undo scan type

Default

The scan type is **passive**.

Views

WLAN RRM view

Default command level

2: System level

Parameters

active: Sets the active scanning mode.

passive: Sets the passive scanning mode.

Examples

Set the scan type to active.

```
<Sysname> system-view
```

```
[Sysname] wlan rrm
[Sysname-wlan-rrm] scan type active
```

wlan rrm

Use **wlan rrm** to enter WLAN RRM view.

Syntax

wlan rrm

Views

System view

Default command level

2: System level

Examples

Enter WLAN RRM view.

```
<Sysname> system-view
[Sysname] wlan rrm
[Sysname-wlan-rrm]
```

WLAN security configuration commands

The terms *AP* and *fat AP* in this document refer to MSR800, MSR 900, MSR900-E, MSR 930, and MSR 20-1X routers with IEEE 802.11b/g and MSR series routers installed with a SIC WLAN module.

WLAN is not available on the following routers:

- MSR 2600.
- MSR 30-11.
- MSR 30-11E.
- MSR 30-11F.
- MSR3600-51F.

authentication-method

Use **authentication-method** to enable an 802.11 authentication method. You can enable open system authentication, shared key authentication or both.

Use **undo authentication-method** to disable the selected authentication method.

Syntax

authentication-method { **open-system** | **shared-key** }

undo authentication-method { **open-system** | **shared-key** }

Default

The open system authentication method is enabled.

Views

Service template view

Default command level

2: System level

Parameters

open-system: Enables open system authentication.

shared-key: Enables shared key authentication.

Examples

Enable open system authentication.

```
<Sysname> system-view
[Sysname] wlan service-template 1 clear
[Sysname-wlan-st-1] authentication-method open-system
```

Enable shared key authentication.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] authentication-method shared-key
```

cipher-suite

Use **cipher-suite** to select the cipher suite used in the encryption of frames.

Use **undo cipher-suite** to disable the selected cipher suite.

Syntax

cipher-suite { **ccmp** | **tkip** | **wep40** | **wep104** | **wep128** }*

undo cipher-suite { **ccmp** | **tkip** | **wep40** | **wep104** | **wep128** }*

Default

No cipher suite is selected.

Views

Service template view

Default command level

2: System level

Parameters

ccmp: Enables the AES-CCMP cipher suite.

tkip: Enables the TKIP cipher suite. TKIP is an encryption mechanism that uses RC4 encryption algorithm and dynamic key management.

wep40: Enables the WEP-40 cipher suite. WEP is an encryption mechanism that uses RC4 encryption algorithm and dynamic key management.

wep104: Enables the WEP-104 cipher suite.

wep128: Enables the WEP-128 cipher suite.

Examples

Enable the TKIP cipher suite.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] cipher-suite tkip
```

gtk-rekey client-offline enable

Use **gtk-rekey client-offline enable** to enable refreshing the Group Temporal Key (GTK) when some client goes offline. This function is effective when GTK rekey is enabled with the **gtk-rekey enable** command.

Use **undo gtk-rekey client-offline** to disable this feature.

Syntax

gtk-rekey client-offline enable

undo gtk-rekey client-offline

Default

The GTK is not refreshed when some client goes off-line.

Views

Service template view

Default command level

2: System level

Examples

Enable GTK rekeying when some client goes off-line.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
```

```
[Sysname-wlan-st-1] gtk-rekey client-offline enable
```

gtk-rekey enable

Use **gtk-rekey enable** to enable GTK rekey.

Use **undo gtk-rekey enable** to disable GTK rekey.

Syntax

gtk-rekey enable

undo gtk-rekey enable

Default

GTK rekey is enabled.

Views

Service template view

Default command level

2: System level

Examples

Disable GTK rekey.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] undo gtk-rekey enable
```

gtk-rekey method

Use **gtk-rekey method** to select a mechanism for re-keying the GTK. If option time-based is selected, the GTK will be refreshed after a specified period of time. If option packet-based is selected, the GTK will be refreshed after a specified number of packets are transmitted.

Use **undo gtk-rekey method** to restore the default.

Syntax

gtk-rekey method { **packet-based** [*packet*] | **time-based** [*time*] }

undo gtk-rekey method

Default

The GTK rekeying method is time-based, and the interval is 86400 seconds.

Views

Service template view

Default command level

2: System level

Parameters

packet-based: Indicates the GTK will be refreshed after a specified number of packets are transmitted.

packet: Number of packets (including multicasts and broadcasts) that are transmitted before the GTK is refreshed. The value is in the range of 5000 to 4294967295 and defaults to 10000000.

time-based: Indicates the GTK will be refreshed based on time.

time: Time after which the GTK is refreshed. The value is in the range of 180 to 604800 seconds defaults to 86400 seconds.

Usage guidelines

The method configured later overwrites the previous one. For example, if you configure the packet-based method and then configure the time-based method, the time-based method is enabled.

Examples

Enable packet-based GTK rekeying and the packet number is 60000.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] gtk-rekey method packet-based 60000
```

ptk-lifetime

Use **ptk-lifetime** to configure the Pairwise Transient Key (PTK) lifetime.

Use **undo ptk-lifetime** to restore the default.

Syntax

ptk-lifetime *time*

undo ptk-lifetime

Default

The PTK lifetime is 43200 seconds.

Views

Service template view

Default command level

2: System level

Parameters

time: Time in the range of 180 to 604800 seconds.

Examples

Specify the PTK lifetime as 86400 seconds.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] ptk-lifetime 86400
```

security-ie

Use **security-ie** to enable the WPA-IE, RSN-IE, or both in the beacon and probe responses.

Use **undo security-ie** to disable the WPA-IE or RSN-IE in the beacon and probe responses.

Syntax

security-ie { **rsn** | **wpa** }

undo security-ie { **rsn** | **wpa** }

Default

Both WPA-IE and RSN-IE are disabled.

Views

Service template view

Default command level

2: System level

Parameters

rsn: Enables the Robust Security Network (RSN) information element in the beacon and probe response frames sent by the AP. The RSN IE advertises the RSN capabilities of the AP.

wpa: Enables the Wi-Fi Protected Access (WPA) Information element in the beacon and probe response frames sent by the AP. The WPA IE advertises the WPA capabilities of the AP.

Examples

Enable the WPA-IE in the beacon and probe responses.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] security-ie wpa
```

tkip-cm-time

Use **tkip-cm-time** to set the TKIP countermeasure time.

Use **undo tkip-cm-time** to restore the default.

Syntax

tkip-cm-time *time*

undo tkip-cm-time

Default

The TKIP counter measure time is 0 seconds. No counter measures are taken.

Views

Service template view

Default command level

2: System level

Parameters

time: TKIP counter measure time in seconds. The value is in the range of 0 to 3600 seconds.

Usage guidelines

After TKIP countermeasures are enabled, if more than two MIC failures occur within a certain time, the TKIP associations are disassociated, and new associations are allowed to establish only after the specified TKIP counter measure time expires.

Examples

Set the TKIP counter measure time to 90 seconds.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] tkip-cm-time 90
```

wep default-key

Use **wep default-key** to configure the WEP default key.

Use **undo wep default-key** to delete the configured WEP default key.

Syntax

wep default-key *key-index* { **wep40** | **wep104** | **wep128**} { **pass-phrase** | **raw-key** } [**cipher** | **simple**] *key*

undo wep default-key *key-index*

Default

The WEP default key index number is 1.

Views

Service template view

Default command level

2: System level

Parameters

key-index: The key index values can be:

1: Configures the 1st WEP default key.

2: Configures the 2nd WEP default key.

3: Configures the 3rd WEP default key.

4: Configures the 4th WEP default key.

wep40: Indicates the WEP40 key option.

wep104: Indicates the WEP104 key option.

wep128: Indicates the WEP128 key option.

pass-phrase: Inputs a character-string pre-shared key.

raw-key: Inputs a hexadecimal-string pre-shared key.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key. This key will be saved in cipher text for security purposes.

string-key: Specifies the key string. The length of a ciphertext key is in the range of 24 to 88 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string. The length of a plaintext key depends on the key options selected:

- For **wep40 pass-phrase**, the key length is 5 alphanumeric characters.
- For **wep104 pass-phrase**, the key length is 13 alphanumeric characters.
- For **wep128 pass-phrase**, the key length is 16 alphanumeric characters.
- For **wep40 raw-key**, the key length is a 10-digit hexadecimal number.
- For **wep104 raw-key**, the key length is a 26-digit hexadecimal number.
- For **wep128 raw-key**, the key length is a 32-digit hexadecimal number.

Usage guidelines

When security IE is configured, WEP default key **1** is not allowed for configuration.

For security purposes, all keys, including keys configured in plain text, are saved in cipher text.

Examples

Specify the first WEP default key as a simple text key **12345**.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
```

```
[Sysname-wlan-st-1] wep default-key 1 wep40 pass-phrase simple 12345
```

wep key-id

Use **wep key-id** to specify the default WEP key used in the encryption and decryption of broadcast and multicast frames. There are 4 static keys in WEP. The key index can be 1, 2, 3, or 4. The key corresponding to the specified key index will be used for encrypting and decrypting broadcast and multicast frames.

Use **undo wep key-id** to restore the default.

Syntax

wep key-id { **1** | **2** | **3** | **4** }

undo wep key-id

Default

The key index number is 1.

Views

Service template view

Default command level

2: System level

Parameters

- **1**: Key index 1.
- **2**: Key index 2.
- **3**: Key index 3.
- **4**: Key index 4.

Examples

Specify the index of the key for broadcast/multicast encryption and decryption as 2.

```
<Sysname> system-view
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] wep key-id 2
```

WLAN IDS configuration commands

The terms *AP* and *fat AP* in this document refer to MSR800, MSR 900, MSR900-E, MSR 930, and MSR 20-1X routers with IEEE 802.11b/g and MSR series routers installed with a SIC WLAN module.

WLAN IDS is not available on the following routers:

- MSR 2600.
- MSR 30-11.
- MSR 30-11E.
- MSR 30-11F.
- MSR3600-51F.

WLAN IDS rogue detection configuration commands

wlan device-detection enable

Use **wlan device-detection enable** to configure the AP to operate in hybrid mode.

Use **undo wlan device-detection enable** to restore the default.

Syntax

wlan device-detection enable

undo wlan device-detection enable

Default

The AP operates in normal mode to provide WLAN services.

Views

System view

Default command level

2: System level

Usage guidelines

If the AP operates in monitor mode, the command is invisible.

Before you change the operating mode of the AP, make sure the radios are disabled. Otherwise, you cannot change the operating mode.

If the AP operates in hybrid mode, configure a service template so the AP can provide both WLAN access and rogue detection services.

Examples

Set the hybrid operation mode for the AP.

```
<Sysname> system-view
[Sysname] wlan device-detection enable
```

wlan ids

Use **wlan ids** to enter WLAN IDS view.

Syntax

wlan ids

Views

System view

Default command level

2: System level

Usage guidelines

This view enables you to configure WLAN IDS parameters such as scan parameters and device lists.

Examples

Enter WLAN IDS view.

```
<Sysname> system-view
[Sysname] wlan ids
[Sysname-wlan-ids]
```

wlan work-mode monitor

Use **wlan work-mode monitor** to configure the AP to operate in monitor mode.

Use **undo wlan work-mode monitor** to restore the default.

Syntax

wlan work-mode monitor

undo wlan work-mode monitor

Default

The AP operates in normal mode to provide WLAN services.

Views

System view

Default command level

2: System level

Usage guidelines

If the AP operates in monitor mode, the command is invisible.

Before you change the operating mode of the AP, make sure the radios are disabled. Otherwise, you cannot change the operating mode.

If the AP operates in monitor mode, the AP can only operate as a monitor AP and cannot operate as an access AP, and cannot provide WLAN services.

Examples

Set the monitor operation mode for the AP.

```
<Sysname> system-view
[Sysname] wlan work-mode monitor
```

WLAN IDS attack detection configuration commands

attack-detection enable

Use **attack-detection enable** to enable the WIDS-IPS detection of various DoS attacks.

Use **undo attack-detection enable** to restore the default.

Syntax

attack-detection enable { **all | flood | spoof | weak-iv** }

undo attack-detection enable

Default

No WIDS-IPS detection is enabled.

Views

WLAN IDS view

Default command level

2: System level

Parameters

all: Enables detection of all kinds of attacks.

flood: Enables detection of flood attacks.

spoof: Enables detection of spoof attacks.

weak-iv: Enables weak-IV detection.

Examples

Enable spoof attack detection.

```
<Sysname> system-view
[Sysname] wlan ids
[Sysname-wlan-ids] attack-detection enable spoof
```

display wlan ids history

Use **display wlan ids history** to display the history of attacks detected in the WLAN system. It supports a maximum of 512 entries.

Syntax

display wlan ids history [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the history of attacks.

```
<Sysname> display wlan ids history
 Total Number of Entries: 5
  Flags:
   act = Action Frame             asr = Association Request
   aur = Authentication Request   daf = Deauthentication Frame
   dar = Disassociation Request   ndf = Null Data Frame
   pbr = Probe Request            rar = Reassociation Request
   saf = Spoofed Disassociation Frame
   sdf = Spoofed Deauthentication Frame
   wiv = Weak IV Detected
   AT - Attack Type, Ch - Channel Number, AR - Average RSSI
                            WIDS History Table
--------------------------------------------------------------------------
 MAC Address      AT    Ch    AR    Detected Time          AP
--------------------------------------------------------------------------
 0027-E699-CA71   asr   8     44    2011-06-12/19:47:54    ap12
 0015-E9A4-D7F4   wiv   8     45    2011-06-12/19:45:28    ap48
 0027-E699-CA71   asr   8     20    2011-06-12/19:18:17    ap12
 003d-B5A6-539F   pbr   8     43    2011-06-12/19:10:48    ap56
 0015-E9A4-D7F4   wiv   8     50    2011-06-12/19:01:28    ap48
--------------------------------------------------------------------------
```

Table 15 Command output

Field	Description
MAC-Address/BSSID	In case of spoof attacks, this field provides the BSSID which was spoofed. In case of other attacks, this field provides the MAC address of the device which initiated the attack.
AT	Type of attack.
Ch	Channel in which the attack was detected.
AR	Average RSSI of the attack frames.
Detected time	Time at which this attack was detected.
AP	Name of the AP that detected this attack.

display wlan ids statistics

Use **display wlan ids statistics** to display the count of attacks detected.

Syntax

display wlan ids statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display WLAN IDS statistics.

```
<Sysname> display wlan ids statistics
 Current attack tracking since: 2011-06-21/12:46:33
------------------------------------------------------------------------
 Type                                          Current       Total
------------------------------------------------------------------------
 Probe Request Frame Flood Attack              2             7
 Authentication Request Frame Flood Attack     0             0
 Deauthentication Frame Flood Attack           0             0
 Association Request Frame Flood Attack        1             1
 Disassociation Request Frame Flood Attack     4             8
 Reassociation Request Frame Flood Attack      0             0
 Action Frame Flood Attack                     0             0
 Null Data Frame Flood Attack                  0             0
 Weak IVs Detected                             12            21
 Spoofed Deauthentication Frame Attack         0             0
 Spoofed Disassociation Frame Attack           0             2
------------------------------------------------------------------------
```

Table 16 Command output

Field	Description
Current	Provides the count of attacks detected since the time specified by the current attack tracking time (specified in the field "Current attack tracking since:"). The current attack tracking time is started at the system startup and is refreshed each hour subsequently.
Total	Provides the total count of the attacks detected since the system startup.
Probe Request Frame Flood Attack	Number of probe request frame flood attacks detected.
Authentication Request Frame Flood Attack	Number of authentication request frame flood attack detected.
Deauthentication Frame Flood Attack	Number of de-authentication frame flood attacks detected.
Association Request Frame Flood Attack	Number of association request frame flood attacks

Field	Description
	detected.
Disassociation Request Frame Flood Attack	Number of disassociation request frame flood attacks detected.
Reassociation Request Frame Flood Attack	Number of reassociation request frame flood attacks detected.
Action Frame Flood Attack	Number of action frame flood attacks detected.
Null Data Frame Flood Attack	Number of null data frame flood attacks detected.
Weak IVs Detected	Number of weak IVs detected.
Spoofed Deauthentication Frame Attack	Number of spoofed deauthentication frame attacks detected.
Spoofed Disassociation Frame Attack	Number of spoofed disassociation frame attacks detected.

reset wlan ids history

Use **reset wlan ids history** to clear the history information of attacks detected in the WLAN.

Syntax

reset wlan ids history

Views

User view

Default command level

1: Monitor level

Usage guidelines

After this command is executed, all the history information regarding attacks will be cleared, and the history table will be empty.

Examples

Clear all history information of attacks.

```
<Sysname> reset wlan ids history
```

reset wlan ids statistics

Use **reset wlan ids statistics** to clear the statistics of attacks detected in the WLAN system.

Syntax

reset wlan ids statistics

Views

User view

Default command level

1: Monitor level

Usage guidelines

This command clears both the "current" and "total" of all attack types in the WLAN IDS statistics table.

Examples

Clear WLAN IDS statistics.

```
<Sysname>reset wlan ids statistics
```

Blacklist and whitelist configuration commands

display wlan blacklist

Use **display wlan blacklist** to display the static or dynamic blacklist entries.

Syntax

display wlan blacklist { **static** | **dynamic** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

static: Displays static blacklist entries.

dynamic: Displays dynamic blacklist entries.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display information about the static blacklist.

```
<Sysname> display wlan blacklist static
Total Number of Entries: 3
                              Static Blacklist
--------------------------------------------------------------------------
 MAC-Address
--------------------------------------------------------------------------
 0014-6c8a-43ff
 0016-6F9D-61F3
 0019-5B79-F04A
--------------------------------------------------------------------------
```

Table 17 Command output

Field	Description
MAC-Address	MAC addresses of clients.

Display information about the dynamic blacklist.

```
<Sysname> display wlan blacklist dynamic
```

```
Total Number of Entries: 3
                              Dynamic Blacklist
--------------------------------------------------------------------------------
 MAC-Address    APID Lifetime(s) Last Updated Since(hh:mm:ss) Reason
--------------------------------------------------------------------------------
 000f-e2cc-0001 1    60          00:02:11                     Assoc-Flood
 000f-e2cc-0002 2    60          00:01:17                     Deauth-Flood
 000f-e2cc-0003 3    60          00:02:08                     Auth-Flood
```

Table 18 Command output

Field	Description
MAC-Address	MAC address of the device inserted into the dynamic blacklist.
APID	AP ID of the corresponding entry in the dynamic blacklist.
Lifetime(s)	Lifetime of the corresponding entry in seconds.
Last Updated Since(hh:mm:ss)	Time elapsed since the entry was updated most recently.
Reason	Reason why the entry was added into the dynamic blacklist.

display wlan whitelist

Use **display wlan whitelist** to display the configured white list.

Syntax

display wlan whitelist [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the white list.

```
<Sysname> display wlan whitelist
Total Number of Entries: 3
                              Whitelist
--------------------------------------------------------------------------------
 MAC-Address
--------------------------------------------------------------------------------
 000e-35b2-000e
```

```
 0019-5b8e-b709
 001c-f0bf-9c92
 0000-0000-00EE
 0400-0000-0000
 0400-0000-00EE
--------------------------------------------------------------------------
```

Table 19 Command output

Field	Description
MAC-Address	MAC addresses of clients in the white list.

dynamic-blacklist enable

Use **dynamic-blacklist enable** to enable the dynamic blacklist feature.

Use **undo dynamic-blacklist enable** to disable the dynamic blacklist feature.

Syntax

dynamic-blacklist enable

undo dynamic-blacklist enable

Default

The dynamic blacklist feature is disabled.

Views

WLAN IDS view

Default command level

2: System level

Parameters

enable: Enables the dynamic blacklist feature.

Usage guidelines

With this feature, a WLAN device, upon detecting flood attacks from a device, adds the device to the dynamic blacklist, and denies any packets from this device until the dynamic blacklist entry ages out.

The maximum number of entries in the dynamic blacklists depends on the device model.

Examples

Enable the dynamic blacklist feature.

```
<Sysname> system-view
[Sysname] wlan ids
[Sysname-wlan-ids] dynamic-blacklist enable
```

dynamic-blacklist lifetime

Use **dynamic-blacklist lifetime** to set the lifetime for dynamic blacklist entries.

Use **undo dynamic-blacklist lifetime** to restore the default.

Syntax

dynamic-blacklist lifetime *lifetime*

undo dynamic-blacklist lifetime

Default

The lifetime is 300 seconds.

Views

WLAN IDS view

Default command level

2: System level

Parameters

lifetime: Interval in the range of 60 to 3600 seconds.

Usage guidelines

If a dynamic blacklist entry is not detected within the lifetime, the entry is removed from the dynamic blacklist.

Examples

Specify a lifetime of 1200 seconds for dynamic blacklist entries.

```
<Sysname> system-view
[Sysname] wlan ids
[Sysname-wlan-ids] dynamic-blacklist lifetime 1200
```

reset wlan dynamic-blacklist

Use **reset wlan dynamic-blacklist** to remove a specified entry or all entries from the dynamic blacklist.

Syntax

reset wlan dynamic-blacklist { **mac-address** *mac-address* | **all** }

Views

User view

Default command level

1: Monitor level

Parameters

mac-address *mac-address*: Removes an entry with the specified MAC address from the dynamic blacklist.

all: Removes all entries from the dynamic blacklist.

Usage guidelines

The maximum number of entries in the dynamic blacklist is 128.

Examples

Remove a client with MAC address 001d-0f31-87d from the dynamic blacklist.

```
<Sysname> reset wlan dynamic-blacklist mac-address 001d-0f31-87d
```

static-blacklist mac-address

Use **static-blacklist mac-address** to add a client with a specified MAC address to the static blacklist.

Use **undo static-blacklist** to remove the client with the specified MAC address or all clients from the static blacklist.

Syntax

static-blacklist mac-address *mac-address*

undo static-blacklist { **mac-address** *mac-address* | **all** }

Views

WLAN IDS view

Default command level

2: System level

Parameters

mac-address: Adds/deletes a client to/from the static blacklist.

all: Deletes all entries from the static blacklist.

Default

No static blacklist exists.

Usage guidelines

Clients in the static blacklist cannot get associated with the AP.

The maximum number of entries in the static blacklist depends on the device model.

Examples

Add the client with MAC address 0014-6c8a-43ff to the static blacklist.

```
<Sysname> system-view
[Sysname] wlan ids
[Sysname-wlan-ids] static-blacklist mac-address 0014-6c8a-43ff
```

whitelist mac-address

Use **whitelist mac-address** to add a client with a specified MAC address to the white list.

Use **undo whitelist** to remove the client with the specified MAC address or all clients from the white list.

Syntax

whitelist mac-address *mac-address*

undo whitelist { **mac-address** *mac-address* | **all** }

Views

WLAN IDS view

Default command level

2: System level

Parameters

mac-address: Adds/deletes the client with the MAC address to/from the white list.

all: Deletes all entries from the white list.

Default

No white list exists.

Usage guidelines

Clients in the white list can be associated with the AP.

The maximum number of entries in the white list depends on the device model.

Examples

Add the client with MAC address 001c-f0bf-9c92 to the white list.

```
<Sysname> system-view
[Sysname] wlan ids
[Sysname-wlan-ids] whitelist mac-address 001c-f0bf-9c92
```

WLAN QoS commands

WLAN is not available on the following routers:

- MSR 2600.
- MSR 30-11.
- MSR 30-11E.
- MSR 30-11F.
- MSR3600-51F.

The terms *AP* and *fat AP* in this document refer to MSR800, MSR 900, MSR900-E, MSR 930, and MSR 20-1X routers with IEEE 802.11b/g and MSR series routers installed with a SIC WLAN module.

client-rate-limit direction (WLAN service-based)

Use **client-rate-limit direction** to configure WLAN service-based client rate limiting.

Use **undo client-rate-limit direction** to restore the default.

Syntax

client-rate-limit direction { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*

undo client-rate-limit direction { **inbound** | **outbound** }

Default

WLAN service-based client rate limiting is disabled.

Views

Service template view

Default command level

2: System level

Parameters

inbound: Specifies the traffic from clients to APs (the outgoing traffic of clients).

outbound: Specifies the traffic from APs to clients (the incoming traffic of clients).

dynamic: Specifies the dynamic mode, where the rate limit for each client is the configured CIR/the number of online clients.

static: Specifies the static mode, where the rate limit for each client is the configured CIR.

cir *cir*: Specifies the rate limit (in kbps) for each client in static mode or specifies the total rate limit for all clients in dynamic mode. This argument ranges from 16 to 300000.

Usage guidelines

WLAN service-based client rate limiting can limit the rate of traffic from clients to APs or the rate of traffic from APs to clients. You can configure client rate limiting for both incoming traffic and outgoing traffic in the same service template.

Examples

Configure WLAN service-based client rate limiting to limit the outgoing traffic rate of each client to 567 kbps and the total incoming traffic rate of all clients to 89 kbps.

```
<Sysname> system-view
[Sysname] wlan service-template 1 clear
[Sysname-wlan-st-1] client-rate-limit direction inbound mode static cir 567
```

```
[Sysname-wlan-st-1] client-rate-limit direction outbound mode dynamic cir 89
```

display wlan client-rate-limit

Use **display wlan client-rate-limit service-template** to display WLAN service-based client rate limiting information.

Syntax

display wlan client-rate-limit service-template [*service-template-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

service-template *service-template-number*: Specifies a service template by its number. If you do not specify a service template, this command displays service-based client rate limiting information of all service templates.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display WLAN service-based client rate limiting information.

```
<Sysname> display wlan client-rate-limit service-template
                            Client Rate Limit
------------------------------------------------------------------------------
 Service Template       Direction       Mode            CIR(kbps)
------------------------------------------------------------------------------
 1                      Inbound         Dynamic         1000
 2                      Outbound        Static          150
 3                      Inbound         Static          300
------------------------------------------------------------------------------
```

Table 20 Command output

Field	Description
Service Template	Service template number.
Direction	Rate-limited direction: • Inbound. • Outbound.
Mode	Rate limiting mode: • Dynamic (shared bandwidth) • Static (exclusive bandwidth)
CIR(kbps)	Rate limit (in kbps)

display wlan wmm

Use **display wlan wmm radio** to display the WMM information of the specified radio or all radios.

Use **display wlan wmm client** to display the WMM information of the client identified by the specified MAC address, of the clients associated with the specified radio, or of all clients.

Syntax

display wlan wmm { **radio** [**interface wlan-radio** *wlan-radio-number*] | **client** { **all** | **interface wlan-radio** *wlan-radio-number* | **mac-address** *mac-address* } } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Default command level

2: System level

Parameters

radio: Displays radio WMM information.

client: Displays client WMM information.

all: Displays WMM information about all clients.

interface wlan-radio *wlan-radio-number*: Specifies a WLAN-radio interface. When the option follows the **radio** keyword, the command displays WMM information of radios connected to the WLAN-radio interface. When the option follows the **client** keyword, the command displays WMM information of clients connected to the WLAN-radio interface.

mac-address *mac-address*: Specifies a client by its MAC address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display the WMM information of all radios.

```
<Sysname> display wlan wmm radio
------------------------------------------------------------------------------
Radio interface : WLAN-Radio2/0
------------------------------------------------------------------------------
Client EDCA update count : 1
 QoS Mode                 : WMM        Radio chip QoS mode      : WMM
 Radio chip max AIFSN     : 255        Radio chip max ECWmin    : 10
 Radio chip max TXOPLimit : 32767      Radio chip max ECWmax    : 10
 CAC Information
  Client accepted               : 0
   Voice                        : 0
   Video                        : 0
  Total request mediumtime(us)  : 0
```

```
  Voice(us)                     : 0
  Video(us)                     : 0
 Calls rejected due to insufficient resource   : 0
 Calls rejected due to invalid parameters      : 0
 Calls rejected due to invalid mediumtime      : 0
 Calls rejected due to invalid delaybound      : 0
QoS Mode                       : WMM
Admission Control Policy       : Users
Threshold users count          : 20
CAC-Free's AC Request Policy   : Response Success
CAC Unauthed Frame Policy      : Downgrade
CAC Medium Time Limitation(us) : 100000
CAC AC-VO's Max Delay(us)      : 50000
CAC AC-VI's Max Delay(us)      : 300000
SVP packet mapped AC number    : Disabled
Radio's WMM Parameters:
                        AC-BK    AC-BE    AC-VI    AC-VO
      ECWmin              4        4        3        2
      ECWmax             10        6        4        3
      AIFSN               7        3        1        1
      TXOPLimit           0        0       94       47
      AckPolicy      Normal   Normal   Normal   Normal
Client's WMM Parameters:
                        AC-BK    AC-BE    AC-VI    AC-VO
      ECWmin              4        4        3        2
      ECWmax             10       10        4        3
      AIFSN               7        3        2        2
      TXOPLimit           0        0       94       47
      CAC           Disable  Disable  Disable  Disable
--------------------------------------------------------------------------------
```

Table 21 Command output

Field	Description
Radio interface	WLAN-Radio interface.
QoS mode	QoS mode: • **WMM**—Indicates that the WMM function is supported. • **none**—Indicates that the WMM function is not supported.
Client EDCA update count	Number of client EDCA parameters updates.
Radio chip WMM support	Indicates whether the radio chip supports the WMM function.
Radio chip max AIFSN	Maximum AIFSN allowed by the radio chip.
Radio chip max ECWMIN	Maximum ECWmin allowed by the radio chip.
Radio chip max TXOPLimit	Maximum TXOPLimit allowed by the radio chip.
Radio chip max ECWMAX	Maximum ECWmax allowed by the radio chip.
Station accepted	Number of stations that have been admitted to

Field	Description
	access the radio.
Voice Mediumtime in use(microsecond per second)	Total medium time of voice traffic (in microseconds per second).
Video Mediumtime in use(microsecond per second)	Total medium time of video traffic (in microseconds per second).
Voice calls in progress	Number of voice calls in progress.
Video calls in progress	Number of video calls in progress.
Calls rejected due to insufficient resource	Number of requests rejected due to insufficient resources.
Calls rejected due to invalid parameters	Number of requests rejected due to invalid parameters.
Calls rejected due to invalid mediumtime	Number of requests rejected due to invalid medium time.
Calls rejected due to invalid delaybound	Number of requests rejected due to invalid delay bound.
Admission Control Policy	Admission control policy.
Threshold users count	Threshold used by the admission control policy.
CAC-Free's AC Request Policy	Response policy used for CAC-incapable ACs.
CAC Unauthed Frame Policy	Policy of processing frames unauthorized by CAC.
CAC Medium Time Limitation(us)	Maximum medium time allowed by the CAC policy (in microseconds).
CAC AC-VO's Max Delay(us)	Maximum voice traffic delay allowed by the CAC policy (in microseconds).
CAC AC-VI's Max Delay(us)	Maximum video traffic delay allowed by the CAC policy (in microseconds).
SVP packet mapped AC number	AC queue to which SVP packets are mapped.
ECWmin	ECWmin value.
ECWmax	ECWmax value.
AIFSN	AIFSN value.
TXOPLimit	TXOPLimit value.
Ack Policy	ACK policy used by an AC queue.
CAC	Indicates whether an AC queue is controlled by CAC: • **Disabled**—Indicates that the AC queue is not controlled by CAC. • **Enabled**—Indicates that the AC queue is controlled by CAC.

Display the WMM information of all the clients.

```
<Sysname> display wlan wmm client all
------------------------------------------------------------------
 MAC address     : 000f-e23c-0000       SSID                : office
 QoS Mode        : None
```

```
-------------------------------------------------------------------
 MAC address     : 000f-e23c-0001       SSID                : office
 QoS Mode        : WMM
 APSD information :
  Max SP Length : all
  L: Legacy      T: Trigger      D: Delivery
  AC             AC-BK   AC-BE   AC-VI   AC-VO
  State          T|D     L       T|D     L
  Assoc State    T|D     L       T|D     T|D
 CAC  information :
  Uplink CAC packets   : 0           Downlink CAC packets   : 0
  Uplink CAC bytes     : 0           Downlink CAC bytes     : 0
  Downgrade packets    : 0           Discard packets        : 0
  Downgrade bytes      : 0           Discard bytes          : 0

  AC                   : AC-VO       User Priority              : 7
   TID                 : 1           Direction             : Bidirectional
   PSB                 : 0           Surplus Bandwidth Allowance : 1.0000
   Medium Time(ms)     : 39.108      Nominal MSDU Size(bytes)    : 1500
   Mean Data Rate(Kbps): 78.125      Minimum PHY Rate(Mbps)      : 2.000
   Create TS time      :  5s
   Update TS time      :  5s
   Uplink TS packets   : 0           Downlink TS packets         : 0
   Uplink TS bytes     : 0           Downlink TS bytes           : 0
```

Table 22 Command output

Field	Description
MAC address	MAC address of a station.
SSID	Service set ID associated with the client.
QoS Mode	QoS mode: • **WMM**—Indicates that the WMM function is supported. • **none**—Indicates that the WMM function is not supported.
Max sp length	Maximum service period.
AC	Access category.
State	APSD attribute of an AC queue: • **T**—Indicates that the AC queue is trigger-enabled. • **D**—Indicates that the AC queue is delivery-enabled. • **T | D**—Indicates that the AC queue is both trigger-enabled and delivery-enabled. • **L**—Indicates that the AC queue is of legacy attributes.
Assoc State	APSD attributes of the four AC queues specified when a client accesses the AP.
Uplink CAC packets	Number of uplink CAC packets.
Uplink CAC bytes	Number of uplink CAC bytes.
Downlink CAC packets	Number of downlink CAC packets.
Downlink CAC bytes	Number of downlink CAC bytes.

Field	Description
Downgrade packets	Number of downgraded packets.
Downgrade bytes	Number of downgraded bytes.
Discard packets	Number of dropped packets.
Discard bytes	Number of dropped bytes.
Direction	Traffic direction.
User Priority	User priority.
TID	Traffic identifier.
PSB	Power saving mode banner.
Nominal MSDU Size(bytes)	Average MSDU size (in bytes).
Mean Data Rate(kbps)	Average data transmission rate (in kbps).
Minimum PHY Rate(Mbps)	Minimum physical transmission rate (in Mbps).
Surplus Bandwidth Allowance	Surplus bandwidth allowance.
Medium Time(ms)	Medium time (in microseconds).
Create TS time	Time from when the TS was created to now.
Update TS time	Time from when the TS was updated to now.
Uplink TS packets	Number of uplink TS packets.
Uplink TS bytes	Number of uplink TS bytes.
Downlink TS packets	Number of downlink TS packets.
Downlink TS bytes	Number of downlink TS bytes.

reset wlan wmm

Use **reset wlan wmm radio** to clear the WMM statistics for the specified radio or all radios.

Use **reset wlan wmm client** to clear the WMM statistics for the client identified by the specified MAC address, the clients associated with the specified radio, or all clients.

Syntax

reset wlan wmm { **radio** [**interface wlan-radio** *wlan-radio-number*] | **client** { **all | interface wlan-radio** *wlan-radio-number* | **mac-address** *mac-address* } }

Views

User view

Default command level

2: System level

Parameters

radio: Clears the WMM statistics for radios.

interface wlan-radio *wlan-radio-number*: Specifies a WLAN-radio interface. When the option follows the **radio** keyword, the command clears WMM information of radios connected to the WLAN-radio interface. When the option follows the **client** keyword, the command clears WMM information of clients connected to the WLAN-radio interface.

client: Clears the WMM statistics for clients.

all: Clears the WMM statistics for all clients.

mac-address *mac-address*: Specifies a client by its MAC address.

Examples

Clear the WMM statistics for all the radios.

```
<Sysname> reset wlan wmm radio all
```

wmm cac policy

Use **wmm cac policy** to configure the access control policy for CAC.

Use **undo wmm cac policy** to restore the default.

Syntax

wmm cac policy { **channelutilization** [*channelutilization-value*] | **users** [*users-number*] }

undo wmm cac policy

Default

The users-based admission policy applies, with the maximum number of admitted users being 20.

Views

WLAN-Radio interface view

Default command level

2: System level

Parameters

channelutilization: Uses the channel utilization-based admission policy for CAC.

channelutilization-value: Maximum channel utilization rate, which specifies the medium time of the accepted AC-VO traffic and AC-VI traffic to the valid time during the unit time. This argument ranges from 0 to 100. It is 65 by default. The unit is % (percentage). The valid time refers to the time available for transmitting and receiving data.

users: Uses the users-based admission policy for CAC.

users-number: Maximum number of clients allowed to be connected, which ranges from 0 to 64. This argument is 20 by default. A client is counted only once, even if it is using both the AC-VO and AC-VI queues.

Examples

Configure CAC to use the channel utilization-based admission policy, with the channel utilization rate being 70%.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio2/0
[Sysname-WLAN-Radio2/0] wmm cac policy channelutilization 70
```

Related commands

wmm edca client

wmm edca radio

Use **wmm edca radio** to set the EDCA parameters and specify the ACK policy.

Use **undo wmm edca radio** to restore the default.

Syntax

wmm edca radio { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **noack** } *

undo wmm edca radio { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** | **ecw** | **txoplimit** | **noack** | **all** }

Default

Normal ACK is used, and the default EDCA parameters are as shown in Table 23.

Table 23 The default EDCA parameters for APs

AC queue	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK queue	7	4	10	0
AC-BE queue	3	4	6	0
AC-VI queue	1	3	4	94
AC-VO queue	1	2	3	47

Views

WLAN-Radio interface view

Default command level

2: System level

Parameters

ac-vo: Specifies the AC-VO (voice traffic) queue.

ac-vi: Specifies the AC-VI (video traffic) queue.

ac-be: Specifies the AC-BE (best-effort traffic) queue.

ac-bk: Specifies the AC-BK (background traffic) queue.

all: Specifies all the EDCA parameters.

noack: Specifies the AC queue to use the No ACK policy. The protocol defines two ACK policies: Normal ACK and No ACK.

txoplimit-value: TXOPLimit parameter of EDCA, which ranges from 0 to 65535 (in units of 32 microseconds). The TXOP value of 0 indicates that only one MPDU can be transmitted. The range of this argument is limited by the radio chip capability.

ecwmin-value: ECWmin parameter of EDCA, which ranges from 0 to 15. The range of this argument is limited by the radio chip capability.

ecwmax-value: ECWmax parameter of EDCA, which ranges from 0 to 15. The range of this argument is limited by the radio chip capability.

aifsn-value: AIFSN parameter of EDCA, which ranges from 1 to 15. The range of this argument is limited by the radio chip capability.

Usage guidelines

For description on each EDCA parameter, see *WLAN Configuration Guide*.

ECWmin must be no greater than ECWmax. The two parameters must be enabled or disabled simultaneously.

When an AP uses 802.11b radio cards, H3C recommends that you set TXOPLimit values of the AC-BK, AC-BE, AC-VI, and AC-VO queues to 0, 0, 188, and 102, respectively.

Examples

Set AIFSN to 2 for the AC-VO queue of the radio.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio2/0
[Sysname-WLAN-Radio2/0] wmm edca radio ac-vo aifsn 2
```

wmm edca client (ac-vo and ac-vi)

Use **wmm edca client** to set EDCA parameters for the AC-BE or AC-BK queue for clients.

Use **undo wmm edca client** to restore the default of the specified or all EDCA parameters for the specified AC queue.

Syntax

wmm edca client { **ac-vo** | **ac-vi** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **cac** } *

undo wmm edca client { **ac-vo** | **ac-vi** } { **aifsn** | **ecw** | **txoplimit** | **cac** | **all** }

Default

The following table lists the default EDCA parameters of the AC-VI and AC-VO queue for clients.

Table 24 Default EDCA parameters for clients

AC queue	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-VI queue	2	3	4	94
AC-VO queue	2	2	3	47

Views

WLAN-Radio interface view

Default command level

2: System level

Parameters

ac-vo: Specifies the AC-VO (voice traffic) queue.

ac-vi: Specifies the AC-VI (video traffic) queue.

all: Specifies all the EDCA parameters.

cac: Enables CAC. The AC-VO and AC-VI queues support CAC, which is disabled by default. The AC-BE and AC-BK queues do not support CAC.

aifsn-value: AIFSN parameter of EDCA, which ranges from 2 to 15.

ecwmin-value: ECWmin parameter of EDCA, which ranges from 0 to 15.

ecwmax-value: ECWmax parameter of EDCA, which ranges from 0 to 15.

txoplimit-value: TXOPLimit parameter of EDCA, which ranges from 0 to 65535 (in units of 32 microseconds). The TXOP value of 0 indicates that only one MPDU can be transmitted.

Usage guidelines

For description on each EDCA parameter, see *WLAN Configuration Guide*.

ECWmin must not be greater than ECWmax. The two parameters must be enabled or disabled simultaneously.

When all the clients are 802.11b terminals, H3C recommends that you set the TXOPLimit to 188 and 102 for the AC-VI and AC-VO queues, respectively.

If both 802.11b and 802.11g clients are present, H3C recommends that you use the default TXOPLimit settings in Table 24.

If CAC is enabled for an AC queue, CAC is also enabled for AC queues with higher priority. For example, if you use the **wmm edca client** command to enable CAC for the AC-VI queue, CAC is also enabled for the AC-VO queue. However, enabling CAC for the AC-VO queue does not enable CAC for the AC-VI queue.

Examples

Set AIFSN to 3 for the AC-VO queue.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio2/0
[Sysname-WLAN-Radio2/0] wmm edca client ac-vo aifsn 3
```

wmm edca client (ac-be and ac-bk)

Use **wmm edca client** to set the EDCA parameters of the AC-VO or AC-VI queue for the clients in a BSS.

Use **undo wmm edca client** to restore the default.

Syntax

wmm edca client { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo wmm edca client { **ac-be** | **ac-bk** } { **aifsn** | **ecw** | **txoplimit** | **all** }

Default

The following table lists the default EDCA parameter settings for the AC-BK and AC-BE queues for clients.

Table 25 Default EDCA parameter settings for clients

AC queue	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK queue	7	4	10	0
AC-BE queue	3	4	10	0

Views

WLAN-Radio interface view

Default command level

2: System level

Parameters

ac-be: Specifies the AC-BE (best-effort traffic) queue.

ac-bk: Specifies the AC-BK (background traffic) queue.

all: Specifies all the EDCA parameters.

aifsn-value: AIFSN parameter of EDCA, in the range of 2 to 15.

ecwmin-value: ECWmin parameter of EDCA, in the range of 0 to 15.

ecwmax-value: ECWmax parameter of EDCA, in the range of 0 to 15.

txoplimit-value: TXOPLimit parameter of EDCA, in the range of 0 to 65535 (in units of 32 microseconds). The TXOP value of 0 indicates that only one MPDU can be transmitted.

Usage guidelines

For description on each EDCA parameter, see *WLAN Configuration Guide*.

ECWmin must not be greater than ECWmax. The two parameters must be enabled or disabled simultaneously.

When all the clients are 802.11b terminals, H3C recommends that you set the TXOPLimit value to 0 for both the AC-BK and AC-BE queues.

If both 802.11b and 802.11g clients are present, H3C recommends that you use the default TXOPLimit settings for the AC-BK and AC-BE queues.

Examples

Set AIFSN to 3 for the AC-BE queue.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio2/0
[Sysname-WLAN-Radio2/0] wmm edca client ac-be aifsn 5
```

wmm enable

Use **wmm enable** to enable the WMM function.

Use **undo wmm enable** to disable the WMM function.

Syntax

wmm enable

undo wmm enable

Default

The WMM function is enabled.

Views

WLAN-Radio interface view

Default command level

2: System level

Usage guidelines

The 802.11n protocol stipulates that all 802.11n clients support WLAN QoS. Therefore, when the radio operates in 802.11an or 802.11gn mode, you should enable WMM. Otherwise, the associated 802.11n clients might fail to communicate.

Examples

Disable the WMM function.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio2/0
[Sysname-WLAN-Radio2/0] undo wmm enable
```

wmm svp map-ac

Use **wmm svp map-ac** to map SVP packets to a specific AC queue.

Use **undo wmm svp map-ac** to restore the default.

Syntax

wmm svp map-ac { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** }

undo wmm svp map-ac

Default

SVP packet mapping is disabled.

Views

WLAN-Radio interface view

Default command level

2: System level

Parameters

ac-vo: Specifies the AC-VO (voice traffic) queue.

ac-vi: Specifies the AC-VI (video traffic) queue.

ac-be: Specifies the AC-BE (best-effort traffic) queue.

ac-bk: Specifies the AC-BK (background traffic) queue.

Usage guidelines

H3C recommends that you map SVP packets to the AC-VO queue in normal cases.

Examples

Map SVP packets to the AC-VO queue.

```
<Sysname> system-view
[Sysname] interface WLAN-Radio2/0
[Sysname-WLAN-Radio2/0] wmm svp map-ac ac-vo
```

Index

S

T

W