H3C MSR Router Series

Comware 5 WLAN Configuration Guide

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

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

Preface

This configuration guide describes fundamentals and configuration of WLAN Interface, WLAN Service, WLAN RRM, WLAN Security, WLAN IDS, and WLAN QoS.

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

Configuring WLAN interfaces

NOTE:

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.

- Wireless routers support WLAN radio interfaces, which are physical interfaces that provide wireless network access.
- Wireless routers support WLAN BSS and WLAN Ethernet virtual interfaces. WLAN radio interfaces on routers can be used as common physical access interfaces. They can be bound to WLAN BSS interfaces and WLAN Ethernet interfaces.

Hardware compatibility with WLAN

WLAN is not available on the following routers:

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

Configuring a WLAN radio interface

WLAN radio interfaces are physical interfaces and are used for providing wireless access service. They can be configured but cannot be removed manually.

To configure a WLAN radio interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN radio interface view.	**interface wlan-radio** *interface-number*	N/A
3. Set the description for the interface.	**description** *text*	Optional. By default, the description of an interface is its interface name followed by the **Interface** string.
4. Specify the expected bandwidth for the interface.	**bandwidth** *bandwidth-value*	Optional.
5. Restore the default settings of the WLAN radio interface.	**default**	Optional.
6. Shut down the WLAN radio interface.	**shutdown**	Optional. By default, a WLAN radio interface is up.

Configuring a WLAN BSS interface

WLAN BSS interfaces are virtual interfaces. They operate like Layer 2 Ethernet ports. A WLAN BSS interface supports multiple Layer 2 protocols. On a wireless router, a WLAN radio interface bound to a WLAN BSS interface operates as a Layer 2 interface.

To configure a WLAN BSS interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN BSS interface view.	**interface wlan-bss** *interface-number*	If the WLAN BSS interface does not exist, this command creates the WLAN BSS interface first. When you bind a service with a WLAN-BSS interface in IMC, make sure the interface number of the WLAN BSS interface is no greater than 31. For more information about IMC, see *H3C Intelligent Management Center Getting Started Guide*.
3. Set the description string for the interface.	**description** *text*	Optional. By default, the description string of an interface is *interface-name* + **Interface**.
4. Specify the link type.	**port link-type** { **access | hybrid** }	Optional. The default is **access**. You can add the WLAN BSS interface to specific VLANs depending on the link type. For more information, see *Layer 2—LAN Switching Configuration Guide*.
5. Specify an authentication domain for MAC authentication users.	**mac-authentication domain** *domain-name*	By default, the default authentication domain is used for MAC authentication users.
6. Set the maximum number of concurrent MAC authentication users on the interface.	**mac-authentication max-user** *user-number*	Optional. The default value is 256.
7. Specify the expected bandwidth for the interface.	**bandwidth** *bandwidth-value*	Optional.
8. Restore the default settings of the WLAN BSS interface.	**default**	Optional.
9. Shut down the WLAN BSS interface.	**shutdown**	Optional. By default, a WLAN BSS interface is up.

For more information about the **mac-authentication domain** and **mac-authentication max-user** commands, see *Security Command Reference*.

WLAN Ethernet interface

WLAN Ethernet interfaces are virtual Layer 3 interfaces. They operate like Layer 3 Ethernet interfaces. You can assign an IP address to a WLAN Ethernet interface. On a wireless router, a WLAN radio interface bound to a WLAN Ethernet interface operates as a Layer 3 interface.

Entering WLAN Ethernet interface view

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN Ethernet interface view.	**interface wlan-ethernet** *interface-number*	If the WLAN Ethernet interface does not exist, this command creates the WLAN Ethernet interface first.
3. Specify the expected bandwidth for the interface.	**bandwidth** *bandwidth-value*	Optional.
4. Restore the default settings of the WLAN Ethernet interface.	**default**	Optional.

Configuring a WLAN Ethernet interface

For a WLAN Ethernet interface, you can configure basic settings such as MTU, ARP, DHCP, and routing protocols as listed in the following table (for information about the commands/features listed in the following table, see related chapters in the corresponding volumes).

To configure a WLAN Ethernet interface:

Step		Command
5. Configure an interface.		• **qos max-bandwidth** • **shutdown** • **mtu** • **description** • **enable snmp trap updown**
6. Configure ARP.		• **arp max-learning-num** • **arp proxy enable** • **proxy-arp enable**
7. Configure the interface as a BOOTP client.		**ip address bootp-alloc**
8. Configure DHCP.	Configure DHCP server	**dhcp select server global-pool**
	Configure DHCP relay	• **dhcp relay address-check** • **dhcp relay information enable** • **dhcp relay information format** • **dhcp relay information strategy** • **dhcp relay release** • **dhcp relay server-select** • **dhcp select relay**
	Configure DHCP client	**ip address dhcp-alloc**
9. Configure IP accounting.		• **ip count firewall-denied**

Step	Command
	• **ip count inbound-packets** • **ip count outbound-packets**
10. Assign an IP address to the interface.	**ip address**
11. Configure IP performance.	• **ip forward-broadcast** • **tcp mss**
12. Configure policy-based routing.	**ip policy-based-route**
13. Configure UDP helper.	**udp-helper server**
14. Configure URPF.	**ip urpf**
15. Configure fast forwarding.	**ip fast-forwarding**
16. Configure basic IPv6 settings.	• **ipv6 address** • **ipv6 address auto link-local** • **ipv6 mtu** • **ipv6 nd autoconfig managed-address-flag** • **ipv6 nd autoconfig other-flag** • **ipv6 nd dad attempts** • **ipv6 nd ns retrans-timer** • **ipv6 nd nud reachable-time** • **ipv6 nd ra halt** • **ipv6 nd ra interval** • **ipv6 nd ra prefix** • **ipv6 nd ra router-lifetime** • **ipv6 neighbors max-learning-num** • **ipv6 policy-based-route**
17. Configure NAT-PT.	**natpt enable**
18. Configure IS-IS.	• **isis authentication-mode** • **isis circuit-level** • **isis circuit-type p2p** • **isis cost** • **isis dis-name** • **isis dis-priority** • **isis enable** • **isis mesh-group** • **isis small-hello** • **isis timer csnp** • **isis timer hello** • **isis timer holding-multiplier** • **isis timer lsp** • **isis timer retransmit** • **isis silent**
19. Configure OSPF.	• **ospf authentication-mode simple** • **ospf authentication-mode** • **ospf cost** • **ospf dr-priority** • **ospf mtu-enable** • **ospf network-type** • **ospf timer dead** • **ospf timer hello**

Step		Command
		• **ospf timer poll** • **ospf timer retransmit** • **ospf trans-delay**
20. Configure RIP.		• **rip authentication-mode** • **rip input** • **rip output** • **rip metricin** • **rip metricout** • **rip poison-reverse** • **rip split-horizon** • **rip summary-address** • **rip version**
21. Configure IPv6 IS-IS.		**isis ipv6 enable**
22. Configure IPv6 OSPFv3.		• **ospfv3 cost** • **ospfv3 mtu-ignore** • **ospfv3 timer dead** • **ospfv3 timer hello** • **ospfv3 timer retransmit** • **ospfv3 area** • **ospfv3 dr-priority** • **ospfv3 trans-delay**
23. Configure IPv6 RIPng.		• **ripng default-route** • **ripng enable** • **ripng metricin** • **ripng metricout** • **ripng poison-reverse** • **ripng split-horizon** • **ripng summary-address**
24. Configure basic MPLS capabilities.		• **mpls** • **mpls ldp** • **mpls ldp advertisement** • **mpls ldp timer hello-hold** • **mpls ldp timer keepalive-hold** • **mpls ldp transport-address**
25. Configure BGP/MPLS VPN.		**ip binding vpn-instance**
26. Configure PPPoE.		• **pppoe-server bind virtual-template** • **pppoe-client dial-bundle-number**
27. Configure bridge sets.		**bridge-set**
28. Configure multicast.	Configure multicast routing and forwarding	• **multicast minimum-ttl** • **multicast ipv6 minimum-hoplimit** • **multicast boundary** • **multicast ipv6 boundary**
	Configure IPv6 multicast routing and forwarding	• **multicast ipv6 minimum-hoplimit** • **multicast ipv6 boundary**
	Configure IGMP	• **igmp enable** • **igmp fast-leave** • **igmp group-policy**

Step		Command
		• **igmp last-member-query-interval** • **igmp max-response-time** • **igmp require-router-alert** • **igmp robust-count** • **igmp send-router-alert** • **igmp static-group** • **igmp timer other-querier-present** • **igmp timer query** • **igmp version**
	Configure MLD	• **mld enable** • **mld last-listener-query-interval** • **mld max-response-time** • **mld require-router-alert** • **mld send-router-alert** • **mld robust-count** • **mld timer other-querier-present** • **mld timer query** • **mld version** • **mld static-group** • **mld group-policy** • **mld fast-leave**
	Configure PIM	• **pim bsr-boundary** • **pim hello-option** • **pim holdtime** • **pim require-genid** • **pim sm** • **pim dm** • **pim state-refresh-capable** • **pim timer graft-retry** • **pim timer hello** • **pim timer join-prune** • **pim triggered-hello-delay**
	Configure IPv6 PIM	• **pim ipv6 bsr-boundary** • **pim ipv6 hello-option** • **pim ipv6 holdtime** • **pim ipv6 require-genid** • **pim ipv6 sm** • **pim ipv6 dm** • **pim ipv6 state-refresh-capable** • **pim ipv6 timer graft-retry** • **pim ipv6 timer hello** • **pim ipv6 timer join-prune** • **pim ipv6 triggered-hello-delay**
29. Configure QoS.	Configure traffic policing, traffic shaping, and line rate	• **qos car** • **qos gts any cir** • **qos gts acl**
	Apply a QoS policy	**qos apply policy**
	Configure congestion avoidance	**qos max-bandwidth**

Step	Command
30. Configure firewall.	• **firewall ethernet-frame-filter** • **firewall packet-filter** • **firewall packet-filter ipv6** • **firewall aspf**
31. Configure NAT.	• **nat outbound** • **nat outbound static** • **nat server**
32. Configure Portal.	• **portal auth-network** • **portal server**
33. Configure IPsec.	**ipsec policy**
34. Configure the backup center.	• **standby interface** • **standby threshold** • **standby timer delay** • **standby timer flow-check** • **standby bandwidth**
35. Configure NetStream.	**ip netstream**
36. Configure NTP.	• **ntp-service broadcast-client** • **ntp-service broadcast-server** • **ntp-service multicast-client** • **ntp-service multicast-server** • **ntp-service in-interface disable**
37. Configure IPX.	**ipx encapsulation**
38. Configure port security.	• **port-security authorization ignore** • **port-security max-mac-count** • **port-security port-mode { mac-and-psk | mac-authentication | mac-else-userlogin-secure | mac-else-userlogin-secure-ext | psk | userlogin-secure | userlogin-secure-ext | userlogin-secure-ext-or-psk | userlogin-secure-or-mac | userlogin-secure-or-mac-ext }** • **port-security preshared-key { pass-phrase | raw-key }** • **port-security tx-key-type 11key**

Displaying and maintaining a WLAN interface

Task	Command	Remarks
Display information about WLAN radio interfaces.	**display interface** [**wlan-radio**] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*] **display interface wlan-radio** *interface-number* [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display information about WLAN BSS interfaces.	**display interface** [**wlan-bss**] [**brief** [**down**]] [**|** { **begin** |	Available in any view.

Task	Command	Remarks
	exclude | **include** } *regular-expression*] **display interface wlan-bss** *interface-number* [**brief**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	
Display information about WLAN Ethernet interfaces.	**display interface** [**wlan-ethernet**] [**brief** [**down**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*] **display interface wlan-ethernet** *interface-number* [**brief**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

Configuring WLAN access

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 access overview

A WLAN can provide the following services:

- WLAN client connectivity to conventional 802.3 LANs
- Secured WLAN access with different authentication and encryption methods
- Seamless roaming of WLAN clients in the mobility domain

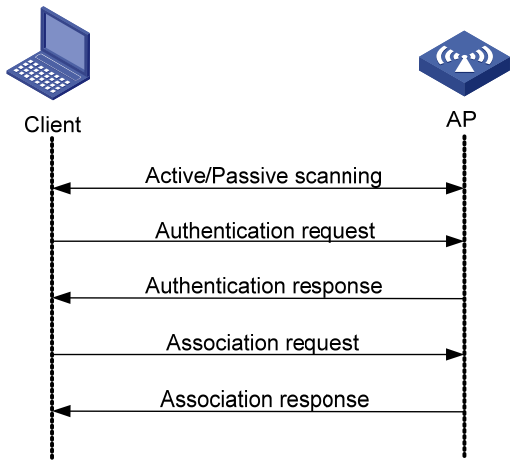
Terminology

- **Client**—A handheld computer or laptop with a wireless NIC or a terminal that supports WiFi.
- **Access point**—An AP bridges frames between wireless and wired networks.
- **Fat AP**—A fat AP controls and manages all associated wireless stations and bridges frames between wired and wireless networks.
- **Service set identifier**—A client scans all networks at first, and then selects a specific SSID to connect to a specific wireless network.
- **Wireless medium**—A medium used for transmitting frames between wireless clients. Radio frequency is used as the wireless medium in the WLAN system.

Client access

A wireless client access process involves three steps: active/passive scanning surrounding wireless services, authentication, and association, as shown in Figure 1.

Figure 1 Establishing a client access



Scanning

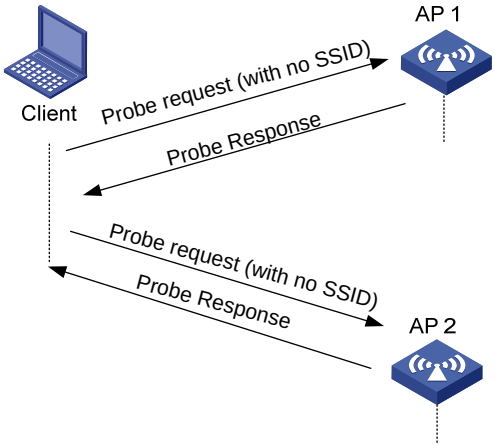
When a wireless client is operating, it usually uses both passive scanning and active scanning to get information about surrounding wireless networks.

1. Active scanning

When a wireless client operates, it periodically searches for (scans) surrounding wireless networks. During active scanning, the wireless client actively sends probe request frames and obtains network signals from received probe response frames. Active scanning includes two modes according to whether a specified SSID is carried in a probe request.

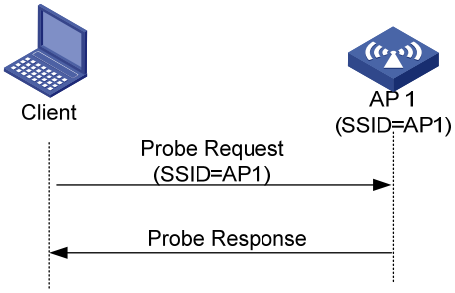
- **A client sends a probe request (with the SSID null, or, the SSID IE length is 0)**—The client periodically sends a probe request frame on each of its supported channels to scan wireless networks. APs that receive the probe request send a probe response, which carries the available wireless network information. The client associates with the AP with the strongest signal. The active scanning mode enables a client to actively get acquainted with the available wireless services and to access the proper wireless network as needed. The active scanning process of a wireless client is as shown in Figure 2.

  Figure 2 Active scanning (the SSID of the probe request is null or no SSID information is carried)



- **A client sends a probe request (with a specified SSID)**—When the wireless client is configured to access a specific wireless network or has already successfully accessed a wireless network, the client periodically sends a probe request carrying the specified SSID of the configured or connected wireless network. When an AP that can provide the wireless service with the specified SSID receives the probe request, it sends a probe response. This active scanning mode enables a client to access a specified wireless network. The active scanning process is as shown in Figure 3.

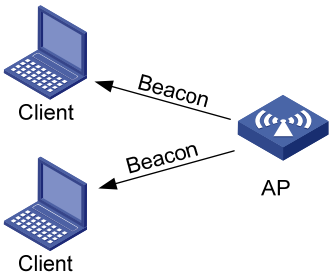
  Figure 3 Active scanning (the probe request carries the specified SSID AP 1)



2. Passive scanning

Passive scanning is used by clients to discover surrounding wireless networks through listening to the beacon frames periodically sent by an AP. All APs providing wireless services periodically send beacons frames, so that wireless clients can periodically listen to beacon frames on the supported channels to get information about surrounding wireless networks and connect to an AP. Passive scanning is used by a client when it wants to save battery power. Typically, VoIP clients adopt the passive scanning mode. The passive scanning process is as shown in Figure 4.

Figure 4 Passive scanning



Authentication

To secure wireless links, the wireless clients must be authenticated before accessing the AP, and only wireless clients passing the authentication can be associated with the AP. 802.11 links define two authentication mechanisms: open system authentication and shared key authentication.

For more information about the two authentication mechanisms, see "Configuring WLAN security."

Association

A client that wants to access a wireless network through an AP must be associated with that AP. Once the client chooses a compatible network with a specified SSID and passes the link authentication to an AP, it sends an association request frame to the AP. The AP detects the capability information carried in the association request frame, determines the capability supported by the wireless client, and sends an association response to the client to notify the client of the association result. Usually, a client can associate with only one AP at a time, and an association process is always initiated by the client.

Hardware compatibility with WLAN

WLAN is not available on the following routers:

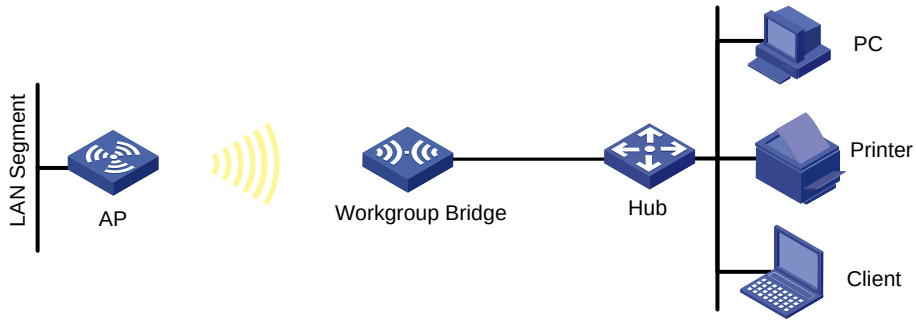
- MSR 2600.
- MSR 30-11.
- MSR 30-11E.
- MSR 30-11F.
- MSR3600-51F.

Workgroup bridge mode overview

The workgroup bridge mode enables an AP to associate with another AP as a wireless client.

As shown in Figure 5, to provide wireless connectivity for the PCs and printer, you can connect them to an AP through a hub or a switch and configure the AP as a workgroup bridge. The PCs and printer access the network through the workgroup bridge.

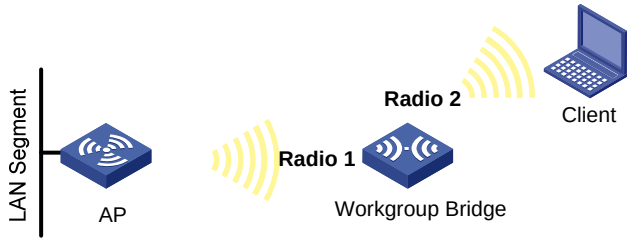
Figure 5 Network diagram



For an AP with two radios, you can configure one radio as a workgroup bridge and configure the other radio to provide normal access services.

As shown in Figure 6, Radio 1 operates as a workgroup bridge, and Radio 2 provides normal access services. Clients associated with Radio 2 can access the network through the workgroup bridge Radio 1.

Figure 6 Dual-radio AP in workgroup bridge mode



WLAN access configuration task list

Task	Description
Specifying a country code	Required.
Configuring a WLAN service template	Required.
Configuring WLAN parameters	Optional.
Configuring radio parameters	Required.

Specifying a country code

A country code identifies the country in which you want to operate radios. It determines characteristics such as operating power level and total number of channels available for the transmission of frames. Set the valid country code or area code before configuring an AP.

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

To specify the country code:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Specify the global country code.	**wlan country-code** *code*	By default, the country code for North American models is US, and for other models is CN.

Configuring a WLAN service template

Creating a service template and specifying an SSID

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a WLAN service template and enter WLAN service template view.	**wlan service-template** *service-template-number* { **clear** | **crypto** }	You cannot change an existing service template to another type.
3. Specify the service set identifier.	**ssid** *ssid-name*	N/A
4. Disable the advertising of SSID in beacon frames.	**beacon ssid-hide**	Optional. By default, the SSID is advertised in beacon frames.

Configuring secure access

WLAN access can be secured by client authentication and data encryption. Client authentication makes sure only authorized users can access the WLAN and data encryption makes sure the data sent can only be received by specific users.

Client authentication includes 802.1X, PSK, and MAC authentication. Data encryption methods include WEP, TKIP, and CCMP.

For more information about WLAN security and port security, see "Configuring WLAN security." For more information about port security, see *Security Configuration Guide*.

To configure secure access:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a WLAN service template and enter WLAN service template view.	**wlan service-template** *service-template-number* { **clear** | **crypto** }	You cannot change an existing service template to another type.
3. Configure an authentication method.	**authentication-method** { **open-system** | **shared-key** }	By default, the open-system authentication method is used. For more information about the command, see *WLAN Command Reference*.

Configuring the maximum number of associated clients

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a WLAN service template and enter WLAN service template view.	**wlan service-template** *service-template-number* { **clear** | **crypto** }	You cannot change an existing service template to another type.
3. Configure the maximum number of clients allowed to associate with a radio.	**client max-count** *max-number*	The default is 32.

Enabling fast association

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a WLAN service template and enter WLAN service template view.	**wlan service-template** *service-template-number* { **clear** | **crypto** }	You cannot change an existing service template to another type.
3. Enable fast association.	**fast-association enable**	By default, fast association is disabled. When this function is enabled, the AP does not perform band navigation or load balancing calculation for clients bound to the SSID.

Enabling a service template

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a WLAN service template and enter WLAN service template view.	**wlan service-template** *service-template-number* { **clear** | **crypto** }	You cannot change an existing service template to another type.
3. Enable the service template.	**service-template enable**	By default, the service template is disabled.

Configuring WLAN parameters

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify the maximum client idle time.	**wlan client idle-timeout** *interval*	Optional. The default is 3600 seconds.
3. Specify the client keepalive interval.	**wlan client keep-alive** *interval*	Optional. By default, the client keep-alive function is disabled.

Step	Command	Remarks
4. Enable the fat AP to respond to probe requests with null SSID.	**broadcast-probe reply**	Optional. The default setting is enabled.

Configuring radio parameters

Configuring radio parameters

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter radio interface view.	**interface wlan-radio** *interface-number*	N/A
3. Configure a radio type.	**radio-type** { **dot11b** | **dot11g** | **dot11gn** }	Optional.
4. Specify a working channel for the radio.	**channel** { *channel-number* | **auto** }	Optional. By default, auto mode is enabled. The working channel of a radio varies with country codes and radio types. The channel list depends on your device model.
5. Specify the maximum radio power.	**max-power** *radio-power*	Optional. By 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.
6. Specify the type of preamble.	**preamble** { **long** | **short** }	Optional. By default, the short preamble is supported.
7. Configure the antenna type.	**antenna type** *type*	Optional. The default setting for the command depends on the device model.
8. Configure the maximum distance that the radio can cover.	**distance** *distance*	Optional. By default, the radio can cover 1 km (0.62 miles) at most.
9. Set the interval for sending beacon frames.	**beacon-interval** *interval*	Optional. By default, the beacon interval is 100 TUs.
10. Set the DTIM counter.	**dtim** *counter*	Optional. By default, the DTIM counter is 1.
11. Specify the maximum length of packets that can be transmitted without fragmentation.	**fragment-threshold** *size*	Optional. By default, the fragment threshold is 2346 bytes and must be an even number.

Step	Command	Remarks
12. Set the maximum number of retransmission attempts for frames larger than the RTS threshold.	**long-retry threshold** *count*	Optional. By default, the long retry threshold is 4.
13. Specify the maximum number of attempts to transmit a frame shorter than the RTS threshold.	**short-retry threshold** *count*	Optional. By default, the short retry threshold is 7.
14. Specify the interval for the AP to hold received packets.	**max-rx-duration** *interval*	Optional. By default, the interval is 2000 milliseconds.
15. Configure collision avoidance	• Specify the request to send (RTS) threshold length. **rts-threshold** *size* • Specify a collision avoidance mechanism. **protection-mode** { **cts-to-self | rts-cts** }	• Optional. By default, the RTS threshold is 2346 bytes. • Optional. By default, the collision avoidance mechanism is CTS-to-Self.

Configuring 802.11n

The following matrix shows the feature and router compatibility:

Feature	MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
802.11n	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.	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n

As the next generation wireless LAN technology, 802.11n supports both 2.4-GHz and 5-GHz bands. It provides higher throughput by using the following methods:

- Increasing bandwidth: 802.11n can bond two adjacent 20-MHz channels together to form a 40-MHz channel. During data forwarding, the two 20-MHz channels can work separately with one acting as the primary channel and the other acting as the secondary channel or working together as a 40-MHz channel. This provides a simple way of doubling the data rate.
- Improving channel utilization through the following ways:
  - 802.11n introduces the A-MPDU frame format. By using only one PHY header, each A-MPDU can accommodate multiple MPDUs which have their PHY headers removed. This reduces the overhead in transmission and the number of ACK frames to be used, and improves network throughput.
  - Similar with MPDU aggregation, multiple MSDU can be aggregated into a single A-MSDU. This reduces the MAC header overhead and improves MAC layer forwarding efficiency.
  - To improve physical layer performance, 802.11n introduces the short GI function, which shortens the GI interval of 800 ns in 802.11a/g to 400 ns. This can increase the data rate by 10 percent.

To configure 802.11n:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter AP template view.	**wlan ap** *ap-name* [**model** *model-name* [**id** *ap-id*]]	Specify the model name only when you create an AP template.
3. Enter radio view.	**radio** *radio-number* **type** { **dot11an** | **dot11gn** }	N/A
4. Specify the bandwidth mode for the radio.	**channel band-width** { **20 | 40** }	Optional. By default, the 802.11gn radio operates in 20 MHz mode.
5. Enable access permission only for 802.11n clients .	**client dot11n-only**	Optional. By default, an 802.11gn radio permits both 802.11b/g and 802.11gn clients to access.
6. Enable the short GI function.	**short-gi enable**	Optional. By default, the short GI function is enabled.
7. Enable the A-MSDU function.	**a-msdu enable**	Optional. By default, the A-MSDU function is enabled. The device receives but does not send A-MSDUs.
8. Enable the A-MPDU function.	**a-mpdu enable**	Optional. By default, the A-MPDU function is enabled.

For information about Modulation and Coding Scheme (MCS) index and mandatory and supported 802.11n rates, see "Configuring WLAN RRM."

Mapping a service template to a radio

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter radio interface view.	**interface wlan-radio** *interface-number*	N/A
3. Configure a radio type.	**radio-type** { **dot11b** | **dot11g** | **dot11gn** }	Optional.
4. Map a service template to the radio.	**service-template** *service-template-number* **interface wlan-bss** *interface-number*	Optional. You can map multiple service templates to the radio. If you use the WLAN BSS interface together with the IMC binding service, make sure the interface number of the WLAN BSS interface is no more than 31. For more information about IMC, see *H3C Intelligent Management Center Getting Started Guide*.

Enabling a radio

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter radio interface view.	**interface wlan-radio** *interface-number*	N/A
3. Enable the radio.	**undo shutdown**	Optional. By default, the radio is disabled.

Displaying and maintaining WLAN access

You can use the **wlan link-test** command to perform a Radio Frequency Ping (RFPing) operation to a client. The operation results show information about signal strength and RTT between the AP and the client.

Task	Command	Remarks
Display WLAN client information.	**display wlan client** { **interface wlan-radio** [*radio-number*] | **mac-address** *mac-address* | **service-template** *service-template-number* } [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display WLAN service template information.	**display wlan service-template** [*service-template-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display WLAN service template information or connection history information.	**display wlan statistics service-template** *service-template-number* [**connect-history**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display WLAN client statistics.	**display wlan statistics client** { **all** | **mac-address** *mac-address* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Cut off clients.	**reset wlan client** { **all** | **mac-address** *mac-address* }	Available in user view.
Clear client statistics.	**reset wlan statistics client** { **all** | **mac-address** *mac-address* }	Available in user view.

Configuring SSID-based access control

When a user wants to access a WLAN temporarily, the administrator can specify a permitted SSID in the corresponding user profile so that the user can only access the WLAN through the SSID.

After completing the configuration, the user profile needs to be enabled to take effect. For more information about user access control, see *Security Configuration Guide*. For more information about user profile, see *Security Configuration Guide*.

To specify a permitted SSID:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter user profile view.	**user-profile** *profile-name*	If the specified user profile does not exist, this command creates it and enters its view.
3. Specify a permitted SSID.	**wlan permit-ssid** *ssid-name*	By default, no permitted SSID is specified, and users can access the WLAN without SSID limitation.
4. Return to system view.	**quit**	N/A
5. Enable the user profile.	**user-profile** *profile-name* **enable**	By default, the user profile is not enabled.

Configuring workgroup bridge mode

Enabling workgroup bridge mode

Follow these guidelines when you enable workgroup bridge mode:

- Do not enable access or WDS service on a radio interface enabled with workgroup bridge mode.
- Do no configure port security on the WLAN-BSS interface enabled with workgroup bridge mode. Otherwise, data cannot be sent or received by the AP.

To enable workgroup bridge mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a WLAN-BSS interface and enter its view.	**interface wlan-bss** *wlan-bss*	N/A
3. Quit to user view.	**quit**	N/A
4. Enter radio interface view.	**interface wlan-radio** *interface-number*	N/A
5. Configure the radio as a workgroup bridge and bind the WLAN-BSS interface to the specified radio.	**client-mode interface wlan-bss** *wlan-bss*	By default, workgroup bridge mode is disabled.

Connecting the workgroup bridge to the wireless network

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a WLAN-BSS interface and enter its view.	**interface wlan-bss** *wlan-bss*	N/A
3. Quit to user view.	**quit**	N/A
4. Enter radio interface view.	**interface wlan-radio** *interface-number*	N/A

Step	Command	Remarks
5. Configure the authentication method for the workgroup bridge.	**client-mode authentication-method** { **open-system** | **shared-key** | **wpa2-psk** }	Optional. By default, open system authentication is used.
6. Configure the cipher suite and pre-shared key for the workgroup bridge.	**client-mode cipher-suite** { **ccmp** | **tkip** | { **wep40** | **wep104** | **wep128** } [**key-id** *key-id*] } **key pass-phrase** [**cipher | simple**] *key*	Optional. By default, no cipher suite or encryption key is configured.
7. Configure the associated SSID for the workgroup bridge.	**client-mode ssid** *ssid*	By default, no associated SSID is configured.
8. Connect the workgroup bridge mode to the wireless network.	**client-mode connect**	Optional.
9. Disconnect the workgroup bridge from the wireless service.	**client-mode disconnect**	Optional.

Displaying and maintaining workgroup bridge

Task	Command	Remarks
Display workgroup bridge configuration and connection status.	**display wlan client-mode radio** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the wireless services scanned by the workgroup bridge and the signal quality.	**display wlan client-mode ssid** [*ssid*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

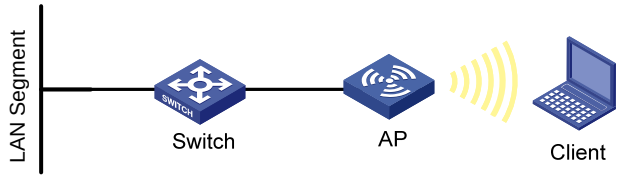
WLAN access configuration examples

WLAN access configuration example

Network requirements

As shown in Figure 7, enable the client to access the internal network resources at any time. The AP provides a plain-text wireless access service with SSID **service**. 802.11g is adopted.

Figure 7 Network diagram



Configuration procedure

1. Configure the fat AP:

Create a WLAN BSS interface.

```
<AP> system-view
```

```
[AP] interface wlan-bss 1
[AP-WLAN-BSS1] quit
```

Configure a clear type WLAN service template, with no authentication.

```
[AP] wlan service-template 1 clear
[AP-wlan-st-1] ssid abc
[AP-wlan-st-1] authentication-method open-system
[AP-wlan-st-1] service-template enable
[AP-wlan-st-1] quit
```

Bind WLAN-Radio 2/0 to service template 1 and WLAN-BSS 1.

```
[AP] interface WLAN-Radio 2/0
[AP-WLAN-Radio2/0] radio-type dot11g
[AP-WLAN-Radio2/0] channel 1
[AP-WLAN-Radio2/0] service-template 1 interface wlan-bss 1
```

2. Verify the configuration:
   - The clients can associate with the APs and access the WLAN.
   - You can use the **display wlan client** command to view the online clients.

802.11n configuration example

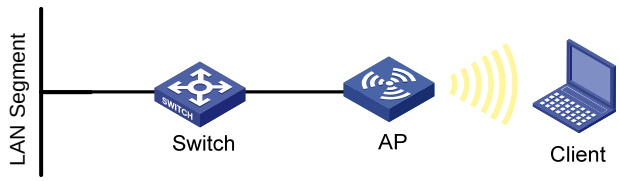
The following matrix shows the feature and router compatibility:

Feature	MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
802.11n	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.	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n

Network requirements

As shown in Figure 8, deploy an 802.11n network to provide high bandwidth access for multi-media applications. The AP provides a plain-text wireless service with SSID **service**. 802.11gn is adopted to inter-work with the existing 802.11g network and protect the current investment.

Figure 8 Network diagram



Configuration procedure

1. Configure the fat AP:

   # Create a WLAN BSS interface.

   ```
   <AP> system-view
   ```

```
[AP] interface wlan-bss 1
[AP-WLAN-BSS1] quit
```

Configure a clear type WLAN service template with no authentication.

```
[AP] wlan service-template 1 clear
[AP-wlan-st-1] ssid service
[AP-wlan-st-1] authentication-method open-system
[AP-wlan-st-1] service-template enable
[AP-wlan-st-1] quit
```

Bind WLAN-Radio 2/0 to service template 1 and WLAN-BSS 1.

```
[AP] interface WLAN-Radio 2/0
[AP-WLAN-Radio2/0] radio-type dot11gn
[AP-WLAN-Radio2/0] service-template 1 interface WLAN-BSS 1
```

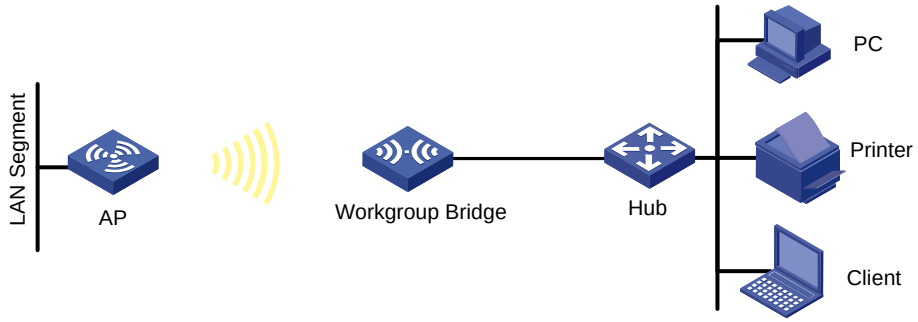
2. Verify the configuration:
   - The clients can associate with the APs and access the WLAN.
   - You can use the **display wlan client verbose** command to view the online clients. The command output displays the 802.11n client information.

Workgroup bridge mode configuration example

Network requirements

As shown in Figure 9, the AP is connected to a LAN, and the workgroup bridge is connected to the AP as a client and is connected to the PCs and printer through its Ethernet port. The workgroup bridge uses the shared-key (WEP) authentication method to access the wireless service China-net.

Figure 9 Network diagram



Configuration procedure

Create a WLAN-BSS interface.

```
<AP> system-view
[AP] interface WLAN-BSS1
[AP-WLAN-BSS1] quit
```

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

```
[AP] interface WLAN-Radio 2/0
[AP-WLAN-Radio2/0] client-mode interface wlan-bss 1
```

Configure the authentication method.

```
[AP-WLAN-Radio2/0] client-mode authentication-method shared-key
```

Configure the cipher suite and pre-shared key.

```
[AP-WLAN-Radio2/0] client-mode cipher-suite wep40 key pass-phrase simple 12345
```

Configure the SSID as China-net.

```
[AP-WLAN-Radio2/0] client-mode ssid China-net
```

Connect the AP to the wireless network.

```
[AP-WLAN-Radio2/0] client-mode connect
[AP-WLAN-Radio2/0] return
```

Verifying the configuration

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

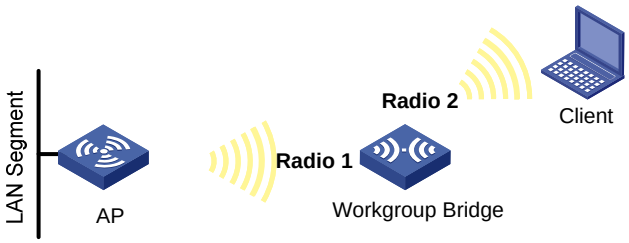
```
<AP> display wlan client-mode radio
                            WLAN Client Mode
--------------------------------------------------------------------------------
 Radio                 : 1
 Mode                  : 802.11g
 Authentication Method : Shared-Key
 Cipher Suite          : WEP40
 Key (Simple)          : 12345
 WEP Key ID            : 1
 SSID                  : China-net
 BSSID                 : 000f-e233-5501
 Status                : Connected
--------------------------------------------------------------------------------
 Received Packets
    Data               : 1324939
    Management         : 34876
 Sent Packets
    Data               : 46365
 Discarded Packets     : 38272
 Rate(Rx/Tx)           : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
 Online Duration       : 0 days 0 hours 45 minutes 5 seconds
 --------------------------------------------------------------------------------
```

The output shows that the AP that operates as a workgroup bridge has been successfully associated with wireless service China-net.

Configuration guidelines

- As shown in Figure 10, the workgroup bridge has two radio interfaces. Radio 1 connects the workgroup bridge to the AP, and Radio 2 connects the workgroup bridge to the client. To enable the client associated with Radio 2 to access the AP through the workgroup bridge, you need to disable wireless user isolation by performing the **wlan-client-isolation enable** command on the workgroup bridge.

  Figure 10 Workgroup bridge with two radio interfaces



- To configure VLAN settings for the uplink wireless interface on the workgroup bridge, make sure the uplink wireless interface has the same VLAN ID as the downlink Ethernet interface on the workgroup bridge.

Configuring WLAN RRM

NOTE:

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.

Overview

Radio signals are susceptible to surrounding interference. The causes of radio signal attenuation in different directions are very complex. Make careful plans before deploying a WLAN network. After WLAN deployment, the running parameters must still be adjusted because the radio environment is always varying due to interference from mobile obstacles, microwave ovens and so on. To adapt to environment changes, radio resources such as working channels and transmit power should be adjusted dynamically. Such adjustments are complex and require experienced personnel to implement regularly, which brings high maintenance costs.

WLAN radio resource management (RRM) is a scalable radio resource management solution. WLAN RRM delivers a real-time, intelligent, and integrated radio resource management solution. This enables a WLAN network to quickly adapt to radio environment changes and remain in a healthy state.

Hardware compatibility with WLAN

WLAN is not available on the following routers:

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

Configuration task list

Task	Remarks
Configuring data transmit rates	Optional
Configuring the maximum bandwidth	Optional
Configuring 802.11g protection	Optional
Configuring 802.11n protection	Optional
Configuring scan parameters	Optional

Configuring data transmit rates

Configuring 802.11b/802.11g rates

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN RRM view.	**wlan rrm**	N/A
3. Configure rates for 802.11b.	**dot11b** { **disabled-rate** | **mandatory-rate** | **multicast-rate** | **supported-rate** } *rate-value*	Optional. By default, no rates are disabled. Mandatory rates are 1 and 2. The multicast rate is automatically selected from mandatory rates. Supported rates are 5.5 and 11.
4. Configure rates for 802.11g.	**dot11g** { **disabled-rate** | **mandatory-rate** | **multicast-rate** | **supported-rate** } *rate-value*	Optional. By default, no rates are disabled. Mandatory rates are 1, 2, 5.5, and 11. The multicast rate is automatically selected from mandatory rates. Supported rates are 6, 9, 12, 18, 24, 36, 48, and 54.

Configuring 802.11n rates

The following matrix shows the feature and router compatibility:

Feature	MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
802.11n	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	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n

Configuration of mandatory and supported 802.11n rates is achieved by specifying the maximum Modulation and Coding Scheme (MCS) index. The MCS data rate table shows relations between data rates, MCS indexes, and parameters that affect data rates. A sample MCS data rate table (20 MHz) is shown in Table 1, and a sample MCS data rate table (40 MHz) is shown in Table 2.

As shown in the two tables, MCS 0 through MCS 7 use one spatial stream, and the data rate corresponding to MCS 7 is the highest; MCS 8 through MCS 15 use two spatial streams, and the data rate corresponding to MCS 15 is the highest.

Table 1 MCS data rate table (20 MHz)

MCS index	Number of spatial streams	Modulation	Data rate (Mbps)	
			800ns GI	400ns GI
0	1	BPSK	6.5	7.2
1	1	QPSK	13.0	14.4
2	1	QPSK	19.5	21.7
3	1	16-QAM	26.0	28.9
4	1	16-QAM	39.0	43.3
5	1	64-QAM	52.0	57.8
6	1	64-QAM	58.5	65.0
7	1	64-QAM	65.0	72.2
8	2	BPSK	13.0	14.4
9	2	QPSK	26.0	28.9
10	2	QPSK	39.0	43.3
11	2	16-QAM	52.0	57.8
12	2	16-QAM	78.0	86.7
13	2	64-QAM	104.0	115.6
14	2	64-QAM	117.0	130.0
15	2	64-QAM	130.0	144.4

Table 2 MCS data rate table (40 MHz)

MCS index	Number of spatial streams	Modulation	Data rate (Mbps)	
			800ns GI	400ns GI
0	1	BPSK	13.5	15.0
1	1	QPSK	27.0	30.0
2	1	QPSK	40.5	45.0
3	1	16-QAM	54.0	60.0
4	1	16-QAM	81.0	90.0
5	1	64-QAM	108.0	120.0
6	1	64-QAM	121.5	135.0
7	1	64-QAM	135.0	150.0
8	2	BPSK	27.0	30.0
9	2	QPSK	54.0	60.0
10	2	QPSK	81.0	90.0
11	2	16-QAM	108.0	120.0
12	2	16-QAM	162.0	180.0
13	2	64-QAM	216.0	240.0
14	2	64-QAM	243.0	270.0

MCS index	Number of spatial streams	Modulation	Data rate (Mbps)	
			800ns GI	400ns GI
15	2	64-QAM	270.0	300.0

802.11 rates include three types: mandatory rates, supported rates, and multicast rates.

- **Mandatory rates**—The AP must support mandatory rates. Clients can only associate with the AP when they support the mandatory rates.
- **Supported rates**—These are higher rates supported by the AP besides the mandatory rates. Supported rates allow some clients that support both mandatory and supported rates to choose higher rates when communicating with the AP.
- **Multicast rates**—These are rates that are supported by the AP besides the mandatory rates. Multicast rates allow clients to send multicast traffic at the multicast rates.

When you specify the maximum MCS index, you actually specify a range. For example, if you specify the maximum MCS index as 5 for mandatory rates, rates corresponding to MCS indexes 0 through 5 are configured as 802.11n mandatory rates.

To configure 802.11n rates:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RRM view.	**wlan rrm**	N/A
3. Specify the maximum MCS index for 802.11n mandatory rates.	**dot11n mandatory maximum-mcs** *index*	Optional. By default, no maximum MCS index is specified for 802.11n mandatory rates. If you configure the **client dot11n-only** command, you must specify the maximum MCS index.
4. Specify the maximum MCS index for 802.11n supported rates.	**dot11n support maximum-mcs** *index*	Optional. By default, the maximum MCS index for 802.11n supported rates is 76.
5. Specify the MCS index for 802.11n multicast rates.	**dot11n multicast-rate** *index*	Optional. By default, the MCS index for 802.11n multicast rates is not specified. Configure the same MCS index settings for APs using 802.11n radios in a mesh network.

Configuring the maximum bandwidth

The following matrix shows the feature and router compatibility:

Feature	MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
802.11n	Available for MSR800-W and	No	Available for MSR900-E-W	Available for MSR 930-W, MSR	Available for routers with a	Available for routers with a	Available for routers with a	Available for routers with a

Feature	MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
	MSR800-10-W			930-W-GU, and MSR 930-W-GT	SIC_WLAN module that supports 802.11n	SIC_WLAN module that supports 802.11n	SIC_WLAN module that supports 802.11n	SIC_WLAN module that supports 802.11n

The configured maximum bandwidth does not take effect on radios enabled with intelligent bandwidth assurance. To validate the configured maximum bandwidth, you must disable the radios and then enable them.

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN RRM view.	**wlan rrm**	N/A
3. Configure the maximum bandwidth.	• 802.11b: **dot11b max-bandwidth** *11b-bandwidth* • 802.11g: **dot11g max-bandwidth** *11g-bandwidth* • 802.11n: **dot11nmax-bandwidth** *11n-bandwidth*	By default: • The maximum bandwidth for 802.11b is 7000 kbps. • The maximum bandwidth for 802.11g is 30000 kbps. • The maximum bandwidth for 802.11n is 180000 kbps. Configure the maximum bandwidth close to and smaller than the upper limit of the actual traffic.

Configuring 802.11g protection

Enabling 802.11g protection

When both 802.11b and 802.11g clients access a WLAN network, interference easily occurs and access rate is greatly degraded because they adopt different modulation modes. To enable both 802.11b and 802.11g clients to operate correctly, enable 802.11g protection for an 802.11g device to send Request to Send/Clear to Send (RTS/CTS) or CTS-to-self (the destination of the CTS packets is the device that sends them) packets to 802.11b devices, which defer access to the medium.

The following cases require 802.11g protection to be enabled on an 802.11g AP.

- An 802.11b client associates with the 802.11g AP. In this case, 802.11g protection is always enabled without manual intervention.
- The 802.11g AP detects an overlapping 802.11b BSS or some 802.11b packets that are not destined to it. To enable 802.11g protection, issue the **dot11g protection enable** command.

To enable 802.11g protection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN RRM view.	**wlan rrm**	N/A
3. Enable 802.11g protection.	**dot11g protection enable**	Optional. By default, 802.11g protection is

Step	Command	Remarks
		disabled. Enabling 802.11g protection reduces network performance.

Configuring 802.11g protection mode

802.11g protection modes include RTS/CTS and CTS-to-self.

- **RTS/CTS**—An AP sends an RTS packet before sending data to a client. After receiving the RTS packet, all the devices within the coverage of the AP do not send data within the specified time. Upon receiving the RTS packet, the client sends a CTS packet. This ensures that all the devices within the coverage of the client do not send data within the specified time.
- **CTS-to-Self**—An AP uses its IP address to send a CTS packet before it sends data to a client. This ensures that all the devices within the coverage of the AP do not send data within the specified time.

To configure the 802.11g protection mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN RRM view.	**wlan rrm**	N/A
3. Configure the 802.11g protection mode.	**dot11g protection-mode** { **cts-to-self** | **rts-cts** }	Optional. By default, the 802.11g protection mode is CTS-to-Self.

Configuring 802.11n protection

The following matrix shows the feature and router compatibility:

Feature	MSR800	MSR 900	MSR900-E	MSR 930	MSR 20-1X	MSR 20	MSR 30	MSR 50
802.11n	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	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n	Available for routers with a SIC_WLAN module that supports 802.11n

Enabling 802.11n protection

When both 802.11n and non 802.11n clients access a WLAN network, interference easily occurs. The access rate is degraded significantly because they adopt different modulation modes. To enable both 802.11n and non-802.11n clients to operate correctly, enable 802.11n protection for an 802.11n device to send RTS/CTS or CTS-to-self (the destination of the CTS packets is the device that sends them) packets to non-802.11n devices, which then defer access to the medium.

The following cases require 802.11n protection to be enabled an 802.11n AP.

- A non-802.11n client associates with the 802.11n AP. In this case, 802.11g protection is always enabled without manual intervention.
- The 802.11n AP detects a non-802.11n BSS or some 802.11n packets that are not destined to it. To enable 802.11n protection, issue the **dot11g protection enable** command.

To enable 802.11n protection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN RRM view.	**wlan rrm**	N/A
3. Enable 802.11n protection.	**dot11n protection enable**	Optional. By default, 802.11n protection is disabled. Enabling 802.11n protection reduces network performance.

Configuring 802.11n protection mode

802.11n protection modes include RTS/CTS and CTS-to-self.

- **RTS/CTS**—An AP sends an RTS packet before sending data to a client. After receiving the RTS packet, all the devices within the coverage of the AP do not send data within the specified time. Upon receiving the RTS packet, the client sends a CTS packet. This ensures that all the devices within the coverage of the client do not send data within the specified time.
- **CTS-to-Self**—An AP uses its IP address to send a CTS packet before it sends data to a client. This ensures that all the devices within the coverage of the AP do not send data within the specified time.

To configure the 802.11n protection mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN RRM view.	**wlan rrm**	N/A
3. Configure the 802.11n protection mode.	**dot11n protection-mode** { **cts-to-self** | **rts-cts** }	Optional. By default, the 802.11n protection mode is CTS-to-Self.

Configuring scan parameters

The **scan type** and **scan report-interval** commands apply to channel adjustment, rogue device detection, and IDS detection.

The **autochannel-set avoid-dot11h** command applies to all types of channel scanning.

To configure scan parameters:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN RRM view.	**wlan rrm**	N/A
3. Set the scan mode.	**scan channel** { **auto** | **all** }	Optional.

Step	Command	Remarks
		By default, the scan mode is auto.
4. Set the scan type.	**scan type** { **active** | **passive** }	Optional. By default, the scan type is **passive**.
5. Set the scan report interval.	**scan report-interval** *seconds*	Optional. By default, the scan report interval is 10 seconds.
6. Configure only non-dot11h channels to be scanned.	**autochannel-set avoid-dot11h**	Optional. By default, the default setting of the command depends on the **scan channel** command.

Displaying and maintaining WLAN RRM

Task	Command	Remarks
Display WLAN RRM information.	**display wlan rrm** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

Configuring WLAN security

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.

Overview

The wireless security incorporated in 802.11 is inadequate for protecting networks that contain sensitive information. They do a fairly good job defending against the general public, but not against good hackers. As a result, there is a need to implement advanced security mechanisms beyond the capabilities of 802.11.

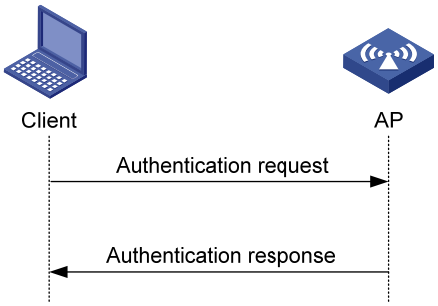
Authentication modes

To secure wireless links, the wireless clients must be authenticated before accessing the AP. Only wireless clients passing the authentication can be associated with the AP. 802.11 links define two authentication mechanisms: open system authentication and shared key authentication.

- Open system authentication

  Open system authentication is the default authentication algorithm. This is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any client that requests authentication with this algorithm can become authenticated. Open system authentication is not required to be successful because an AP may decline to authenticate the client. Open system authentication involves a two-step authentication process. In the first step, the wireless client sends a request for authentication. In the second step, the AP determines if the wireless client passes the authentication and returns the result to the client.

  Figure 11 Open system authentication process

- Shared key authentication

  The following figure shows a shared key authentication process. The two parties have the same shared key configured.

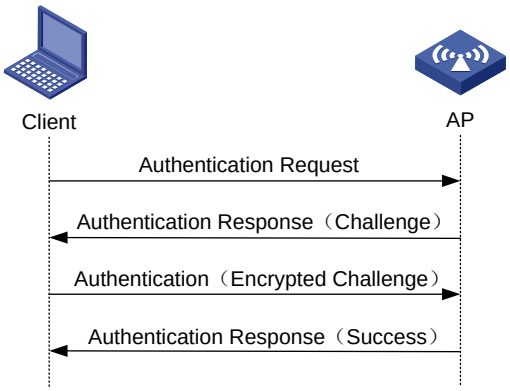
  a. The client sends an authentication request to the AP.

  b. The AP randomly generates a challenge and sends it to the client.

  c. The client uses the shared key to encrypt the challenge and sends it to the AP.

  d. The AP uses the shared key to de-encrypt the challenge and compares the result with that received from the client. If they are identical, the client passes the authentication. If not, the authentication fails.

Figure 12 Shared key authentication process



WLAN data security

Compared with wired networks, WLAN networks are more susceptible to attacks because all WLAN devices share the same medium and thus every device can receive data from any other sending device. Plain-text data is transmitted over the WLAN if there is no security service.

To secure data transmission, 802.11 protocols provide some encryption methods to ensure that devices without the right key cannot read encrypted data.

1. WEP encryption

   Wired Equivalent Privacy (WEP) was developed to protect data exchanged among authorized users in a wireless LAN from casual eavesdropping. WEP uses RC4 encryption (a stream encryption method) for confidentiality and supports WEP40, WEP104, and WEP128 keys. Although WEP encryption increases the difficulty of network interception and session hijacking, it still has weaknesses due to limitations of RC4 encryption algorithm and static key configuration.

2. TKIP encryption

   Temporal key integrity Protocol (TKIP) and WEP both use the RC4 algorithm, but TKIP has several advantages over WEP, and provides more secure protection for WLAN as follows:

   - First, TKIP provides longer IVs to enhance encryption security. Compared with WEP encryption, TKIP encryption uses 128-bit RC4 encryption algorithm, and increases the length of IVs from 24 bits to 48 bits.
   - Second, TKIP allows for dynamic key negotiation to avoid static key configuration. TKIP replaces a single static key with a base key generated by an authentication server. TKIP dynamic keys cannot be easily deciphered.
   - Third, TKIP offers MIC and countermeasures. If a packet fails the MIC, the data might be tampered, and the system might be attacked. If two packets fail the MIC in a certain period, the AP automatically takes countermeasures. It will not provide services in a certain period to prevent attacks.

3. AES-CCMP encryption

   CTR with CCMP is based on the CCM of the AES encryption algorithm. CCM combines CTR for confidentiality and CBC-MAC for authentication and integrity. CCM protects the integrity of both the MAC Protocol Data Unit (MPDU) Data field and selected portions of the IEEE 802.11 MPDU header. The AES block algorithm in CCMP uses a 128-bit key and a 128-bit block size. Similarly, CCMP contains a dynamic key negotiation and management method, so that each wireless client can dynamically negotiate a key suite, which can be updated periodically to further enhance the security of the CCMP encryption mechanism. During the encryption process, CCMP uses a 48-bit packet number (PN) to ensure that each encrypted packet uses a different PN, improving the security to a certain extent.

Client access authentication

1. PSK authentication

   To implement pre-shared key (PSK) authentication, the client and the authenticator must have the same shared key configured. Otherwise, the client cannot pass the PSK authentication.

2. 802.1X authentication

   As a port-based access control protocol, 802.1X authenticates and controls accessing devices at the port level. A device that is connected to an 802.1X-enabled port of a WLAN access control device can access the resources on the WLAN only after passing authentication.

3. MAC address authentication

   MAC address authentication does not require any client software. The MAC address of a client is compared against a predefined list of allowed MAC addresses. If a match is found, the client can pass the authentication and access the WLAN. If no match is found, the authentication fails and access is denied. The entire process does not require the user to enter a username or password. This type of authentication is suited to small networks (such as families and small offices) with fixed clients.

   MAC address authentication can be done locally or through a RADIUS server.

   - **Local MAC address authentication**—A list of usernames and passwords (the MAC addresses of allowed clients) is created on the wireless access device and the clients are authenticated by the wireless access device. Only clients whose MAC addresses are included in the list can pass the authentication and access the WLAN.
   - **MAC address authentication through RADIUS server**—The wireless access device serves as the RADIUS client and sends the MAC address of each requesting client to the RADIUS server. If the client passes the authentication on the RADIUS server, the client can access the WLAN within the authorization assigned by the RADIUS server. In this authentication mode, if different domains are defined, authentication information of different SSIDs are sent to different RADIUS servers based on their domains.

For more information about access authentication, see *Security Configuration Guide*.

Protocols and standards

- **IEEE Standard for Information technology**—Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements -2004
- **WI-FI Protected Access**—Enhanced Security Implementation Based On IEEE P802.11i Standard-Aug 2004
- **Information technology**—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—802.11, 1999
- IEEE Standard for Local and metropolitan area networks "Port-Based Network Access Control" 802.1X™- 2004
- **802.11i IEEE Standard for Information technology**—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements

Hardware compatibility with WLAN

WLAN is not available on the following routers:

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

- MSR3600-51F.

Configuring WLAN security

Configuration task list

To configure WLAN security in a service template, map the service template to a radio policy, and add radios to the radio policy. The SSID name, advertisement setting (beaconing), and encryption settings are configured in the service template. You can configure an SSID to support any combination of WPA, RSN, and Pre-RSN clients

Task	Remarks
Enabling an authentication method	Required
Configuring the PTK lifetime	Optional
Configuring the GTK rekey method	Optional
Configuring security IE	Required
Configuring cipher suite	Required
Configuring port security	Optional

Enabling an authentication method

You can enable open system or shared key authentication or both.

To enable an authentication method:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN service template view.	**wlan service-template** *service-template-number* **crypto**	N/A
3. Enable the authentication method.	**authentication-method** { **open-system** | **shared-key** }	Optional. By default, open system authentication is adopted. • The shared-key authentication can be adopted only when WEP encryption is used, and you must configure the **authentication-method shared-key** command. • For RSN and WPA, the authentication method must be open system authentication.

Configuring the PTK lifetime

A pairwise transient key (PTK) is generated through a four-way handshake, during which, the pairwise master key (PMK), an AP random value (ANonce), a site random value (SNonce), the AP's MAC address and the client's MAC address are used.

To configure the PTK lifetime:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN service template view.	**wlan service-template** *service-template-number* **crypto**	N/A
3. Configure the PTK lifetime.	**ptk-lifetime** *time*	Optional. By default, the PTK lifetime is 43200 seconds.

Configuring the GTK rekey method

A fat AP generates a group temporal key (GTK) and sends the GTK to a client during the authentication process between an AP and the client through group key handshake or the 4-way handshake. The client uses the GTK to decrypt broadcast and multicast packets. The Robust Security Network (RSN) negotiates the GTK through the 4-way handshake or group key handshake, and Wi-Fi Protected Access (WPA) negotiates the GTK only through group key handshake.

Two GTK rekey methods can be configured:

- **Time-based GTK rekey**—After the specified interval elapses, GTK rekey occurs.
- **Packet-based GTK rekey**—After the specified number of packets is sent, GTK rekey occurs.

By default, time-based GTK rekey is adopted, and the rekey interval is 86400 seconds.

Configuring a new GTK rekey method overwrites the previous one. For example, if time-based GTK rekey is configured after packet-based GTK rekey is configured, time-based GTK rekey takes effect.

You can also configure the device to start GTK rekey when a client goes offline.

Configuring GTK rekey based on time

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN service template view.	**wlan service-template** *service-template-number* **crypto**	N/A
3. Enable GTK rekey.	**gtk-rekey enable**	By default, GTK rekey is enabled.
4. Configure the GTK rekey interval.	**gtk-rekey method time-based** [*time*]	By default, the interval is 86400 seconds.
5. Configure the device to start GTK rekey when a client goes offline.	**gtk-rekey client-offline enable**	Optional. By default, the device does not start GTK rekey when a client goes offline. This command takes effect only when you execute the **gtk-rekey enable** command.

Configuring GTK rekey based on packet

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN service template view.	**wlan service-template** *service-template-number* **crypto**	N/A

Step	Command	Remarks
3. Enable GTK rekey.	**gtk-rekey enable**	By default, GTK rekey is enabled.
4. Configure GTK rekey based on packet.	**gtk-rekey method packet-based** [*packet*]	The default packet number is 10000000.
5. Configure the device to start GTK rekey when a client goes offline.	**gtk-rekey client-offline enable**	Optional. By default, the device does not start GTK rekey when a client goes offline. This command takes effect only when you execute the **gtk-rekey enable** command.

Configuring security IE

Security IE configurations comprise WPA security IE configuration and RSN security IE configuration, both of which require open system authentication.

WPA ensures greater protection than WEP. WPA operates in either WPA-PSK (or Personal) mode or WPA-802.1X (or Enterprise) mode. In Personal mode, a pre-shared key or pass-phrase is used for authentication. In Enterprise mode, 802.1X and RADIUS servers and the EAP are used for authentication.

Configuring WPA security IE

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN service template view.	**wlan service-template** *service-template-number* **crypto**	N/A
3. Enable the WPA-IE in the beacon and probe responses.	**security-ie wpa**	By default, WPA-IE is disabled.

Configuring RSN security IE

An RSN is a security network that only allows the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN Information Element (IE) of beacon frames. It provides greater protection than WEP and WPA.

To configure RSN security IE:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN service template view.	**wlan service-template** *service-template-number* **crypto**	N/A
3. Enable the RSN-IE in the beacon and probe responses.	**security-ie rsn**	By default, RSN-IE is disabled.

Configuring cipher suite

A cipher suite is used for data encapsulation and de-encapsulation. It uses the following encryption methods:

- WEP40/WEP104/WEP128
- TKIP
- AES-CCMP

Configuring WEP cipher suite

The WEP encryption mechanism requires that the authenticator and clients on a WLAN have the same key configured. WEP adopts the RC4 algorithm (a stream encryption algorithm), supporting WEP40, WEP104 and WEP128 keys.

You can use WEP with either open system or shared key authentication mode:

- In open system authentication mode, the WEP key is used for encryption only and not for authentication. A client can access the network without having the same key as the authenticator. However, if the receiver has a different key from the sender, it discards the packets received from the sender.
- In shared key authentication mode, the WEP key is used for both encryption and authentication. If the key of a client is different from that of the authenticator, the client cannot pass the authentication and the access of the client is denied.

To configure WEP encryption:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN service template view.	**wlan service-template** *service-template-number* **crypto**	N/A
3. Enable the WEP cipher suite.	**cipher-suite** { **wep40** | **wep104** | **wep128** }	By default, no cipher suite is selected.
4. Configure the WEP default key.	**wep default-key** { **1** | **2** | **3** | **4** } { **wep40** | **wep104** | **wep128** } { **pass-phrase** | **raw-key** } [**cipher** | **simple**] *key*	By default, the WEP default key index number is 1.
5. Specify a key index number.	**wep key-id** { **1** | **2** | **3** | **4** }	Optional. By default, the key index number is that configured with the **wep default-key** command.

Configuring TKIP cipher suite

Message integrity check (MIC) is used to prevent attackers from data modification. It ensures data security by using the Michael algorithm. When a fault occurs to the MIC, the device will consider that the data has been modified and the system is being attacked. Upon detecting the attack, TKIP will suspend within the countermeasure interval. No TKIP associations can be established within the interval.

To configure TKIP cipher suite:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN service template view.	**wlan service-template** *service-template-number* **crypto**	N/A
3. Enable the TKIP cipher suite.	**cipher-suite tkip**	By default, no cipher suite is selected.
4. Configure the TKIP countermeasure interval.	**tkip-cm-time** *time*	Optional. The default countermeasure interval is 0 seconds. No

Step	Command	Remarks
		countermeasures are taken.

Configuring AES-CCMP cipher suite

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN service template view.	**wlan service-template** *service-template-number* **crypto**	N/A
3. Enable the AES-CCMP cipher suite.	**cipher-suite ccmp**	By default, no cipher suite is selected.

Configuring port security

The authentication type configuration includes the following options:

- PSK
- 802.1X
- MAC
- PSK and MAC

This document describes only common port security modes. For more information about other port security modes, see *Security Configuration Guide*.

Before configuring port security, create the wireless port and enable port security.

Configuring PSK authentication

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN-BSS interface view.	**interface wlan-bss** *interface-number*	N/A
3. Enable 802.11 key negotiation.	**port-security tx-key-type 11key**	By default, 802.11 key negotiation is not enabled.
4. Configure the pre-shared key.	**port-security preshared-key** { **pass-phrase** | **raw-key** } [**cipher** | **simple**] *key*	By default, no pre-shared key is configured.
5. Enable the PSK port security mode.	**port-security port-mode psk**	N/A

Configuring 802.1X authentication

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN-BSS interface view.	**interface wlan-bss** *interface-number*	N/A
3. Enable 802.11 key negotiation.	**port-security tx-key-type 11key**	By default, 802.11 key negotiation is not enabled.
4. Enable the 802.1X port security mode.	**port-security port-mode userlogin-secure-ext**	N/A

Configuring MAC address authentication

802.11i does not support MAC address authentication.

To configure MAC address authentication:

Step	Command
1. Enter system view.	**system-view**
2. Enter WLAN-BSS interface view.	**interface wlan-bss** *interface-number*
3. Enable MAC port security mode.	**port-security port-mode mac-authentication**

Configuring PSK and MAC address authentication

For more information about port security configuration commands, see *Security Configuration Guide*.

To configure PSK and MAC address authentication:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN-BSS interface view.	**interface wlan-bss** *interface-number*	N/A
3. Enable 802.11 key negotiation.	**port-security tx-key-type 11key**	By default, 802.11 key negotiation is not enabled.
4. Enable the PSK and MAC port security mode.	**port-security port-mode mac-and-psk**	N/A
5. Configure the pre-shared key.	**port-security preshared-key** { **pass-phrase** | **raw-key** } *key*	The key is a string of 8 to 63 characters, or a 64-digit hex number.

Displaying and maintaining WLAN security

For more information about related **display** commands, see *Security Command Reference*.

Task	Command	Remarks
Display WLAN service template information.	**display wlan service-template** [*service-template-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display MAC address authentication information.	**display mac-authentication** [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the PSK user information of port security.	**display port-security preshared-key user** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the configuration information, running state and statistics of port security.	**display port-security** [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display 802.1X session	**display dot1x** [**sessions |**	Available in any view.

Task	Command	Remarks
information or statistics.	**statistics**] [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	

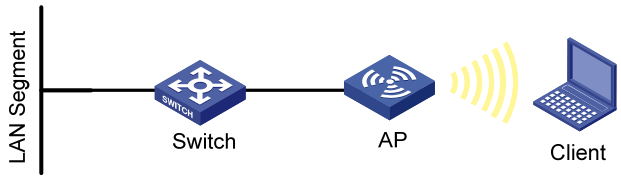
WLAN security configuration examples

PSK authentication configuration example

Network requirements

As shown in Figure 13, perform PSK authentication with key 12345678 on the client.

Figure 13 Network diagram



Configuration procedure

Enable port security.

```
<Sysname> system-view
[Sysname] port-security enable
```

Configure the authentication mode as PSK, and the pre-shared key as **12345678**, and enable 802.11 key negotiation.

```
[Sysname] interface wlan-bss 1
[Sysname-WLAN-BSS1] port-security port-mode psk
[Sysname-WLAN-BSS1] port-security preshared-key pass-phrase 12345678
[Sysname-WLAN-BSS1] port-security tx-key-type 11key
[Sysname-WLAN-BSS1] quit
```

Create crypto-type service template 10 and configure its SSID as **psktest**, configure the authentication method as **open-system**, and enable the service template.

```
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] ssid psktest
[Sysname-wlan-st-1] security-ie rsn
[Sysname-wlan-st-1] cipher-suite ccmp
[Sysname-wlan-st-1] authentication-method open-system
[Sysname-wlan-st-1] service-template enable
[Sysname-wlan-st-1] quit
```

Bind interface WLAN-BSS 1 to service template 1 on interface WLAN-radio 2/0.

```
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] radio-type dot11g
[Sysname-WLAN-Radio2/0] service-template 1 interface wlan-bss 1
```

Verifying the configuration

- After the client has the same PSK configured, it can associate with the AP and access the WLAN.

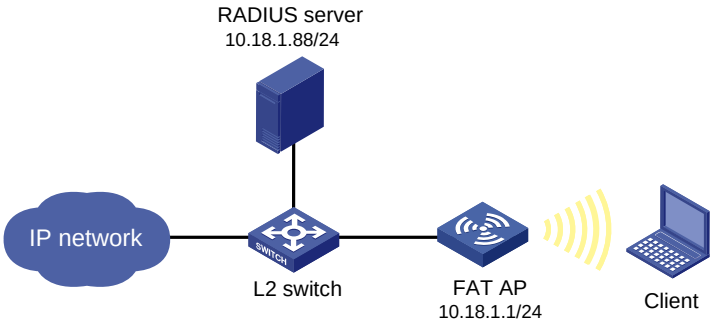
- You can use the **display wlan client** command and **display port-security preshared-key user** command to view the online clients.

MAC and PSK authentication configuration example

Network requirements

As shown in Figure 14, perform MAC and PSK authentication on the client.

Figure 14 Network diagram



Configuring the fat AP

Enable port security.

```
<Sysname> system-view
[Sysname] port-security enable
```

Configure the port mode of the WLAN BSS interface as **mac-and-psk** (with the pre-shared key **12345678**) and enable 802.11key negotiation.

```
[Sysname] interface wlan-bss 1
[Sysname-WLAN-BSS1] port-security port-mode mac-and-psk
[Sysname-WLAN-BSS1] port-security preshared-key pass-phrase 12345678
[Sysname-WLAN-BSS1] port-security tx-key-type 11key
[Sysname-WLAN-BSS1] quit
```

Create service template 2 of crypto type and configure its SSID as **mactest**.

```
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] ssid mactest
```

Enable the RSN-IE in the beacon and probe responses and enable the AES-CCMP cipher suite in the encryption of frames.

```
[Sysname-wlan-st-1] security-ie rsn
[Sysname-wlan-st-1] cipher-suite ccmp
```

Configure the authentication method as open-system and enable the service template.

```
[Sysname-wlan-st-1] authentication-method open-system
[Sysname-wlan-st-1] service-template enable
[Sysname-wlan-st-1] quit
```

Configure the IP addresses of the primary authentication server and accounting server as 10.18.1.88, the shared key for RADIUS authentication/accounting packets as **12345678**, and specify the extended RADIUS server type.

```
[Sysname] radius scheme rad
[Sysname-radius-rad] primary authentication 10.18.1.88
[Sysname-radius-rad] primary accounting 10.18.1.88
[Sysname-radius-rad] server-type extended
```

Configure the shared key for RADIUS authentication/accounting packets as **12345678**.

```
[Sysname-radius-rad] key authentication 12345678
[Sysname-radius-rad] key accounting 12345678
[Sysname-radius-rad] user-name-format without-domain
[Sysname-radius-rad] quit
```

Configure AAA domain **cams** by referencing RADIUS scheme **rad**.

```
[Sysname] domain cams
[Sysname-isp-cams] authentication lan-access radius-scheme rad
[Sysname-isp-cams] authorization lan-access radius-scheme rad
[Sysname-isp-cams] accounting lan-access radius-scheme rad
[Sysname-isp-cams] quit
```

Configure the MAC address authentication domain as **cams**.

```
[Sysname] mac-authentication domain cams
```

Configure MAC address authentication user name format, using MAC addresses without hyphen as username and password (consistent with the format on the server).

```
[Sysname] mac-authentication user-name-format mac-address without-hyphen
```

On interface WLAN-radio 2/0, bind interface WLAN-BSS 1 to service template 1.

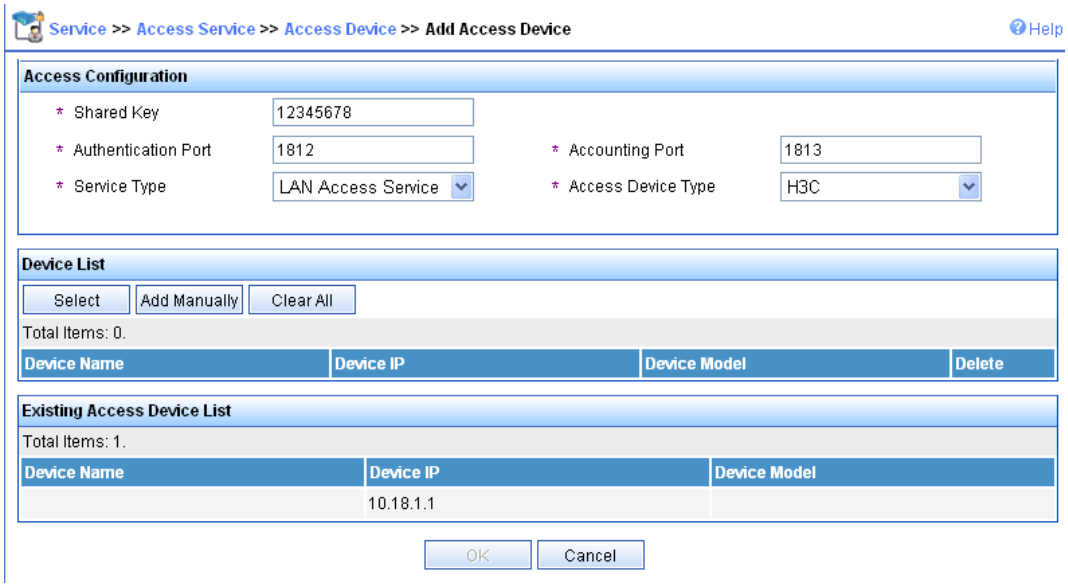
```
[Sysname] interface wlan-radio2/0
[Sysname-WLAN-Radio2/0] radio-type dot11g
[Sysname-WLAN-Radio2/0] service-template 1 interface wlan-bss 1
```

Configuring the RADIUS server (IMCv3)

The following takes the IMC (the IMC versions are IMC PLAT 3.20-R2602 and IMC UAM 3.60-E6102) as an example to illustrate the basic configurations of the RADIUS server.

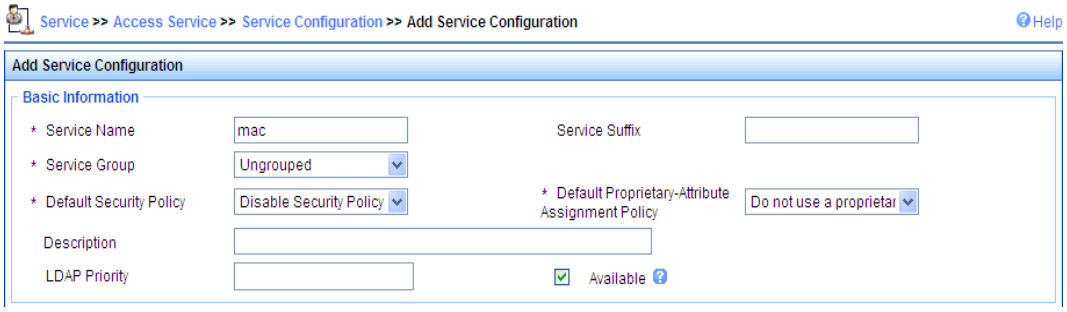
1. Add an access device:
   a. Click the **Service** tab.
   b. Select **Access Service** > **Access Device** from the navigation tree.
   c. Click **Add**.
   d. On the page that appears, enter **12345678** for **Shared Key**, add ports **1812**, and **1813** for **Authentication Port** and **Accounting Port,** respectively, select **LAN Access Service** for **Service Type**, select **H3C** for **Access Device Type**, and select or manually add an access device with the IP address 10.18.1.1, and click **Apply**.

Figure 15 Adding an access device



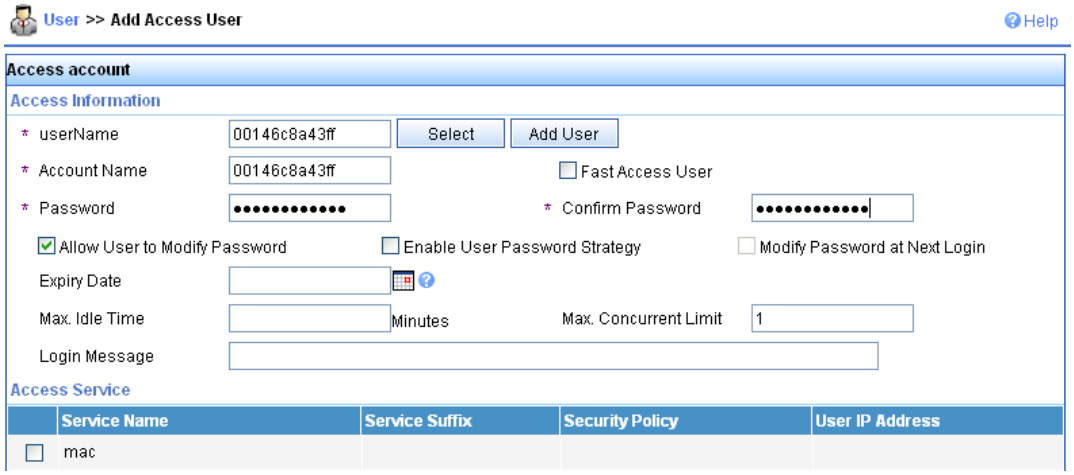
2. Add a service:
   a. Click the **Service** tab.
   b. Select **Access Service** > **Access Device** from the navigation tree.
   c. Click **Add**.
   d. On the page that appears, set the service name to **mac**, keep the default values for other parameters, and click **Apply**.

Figure 16 Adding a service



3. Add an account:
   a. Click the **User** tab.
   b. Select **User** > **All Access Users** from the navigation tree.
   c. Click **Add**.
   d. On the page that appears, enter a username **00146c8a43ff**, enter an account and password **00146c8a43ff**, select the service **mac**, and click **Apply**.

Figure 17 Adding an account

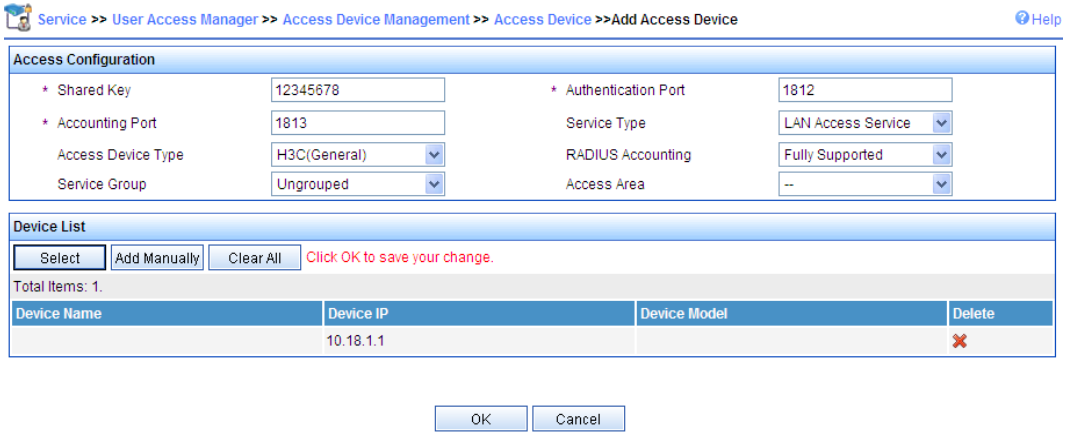


Configuring the RADIUS server (IMCv5)

The following takes the IMC (the IMC versions are IMC PLAT 5.0 and IMC UAM 5.0) as an example to illustrate the basic configurations of the RADIUS server.

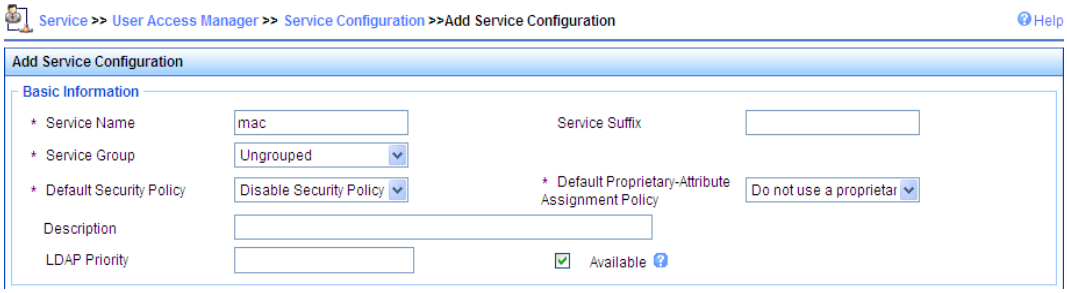
1. Add an access device:
   a. Click the **Service** tab in the IMC platform.
   b. Select **User Access Manager** > **Access Device Management** from the navigation tree.
   c. Click **Add**.
   d. On the page that appears, enter **12345678** as the **Shared Key**, keep the default values for other parameters, and select or manually add the access device with the IP address 10.18.1.1, and click **Apply**.

Figure 18 Adding an access device



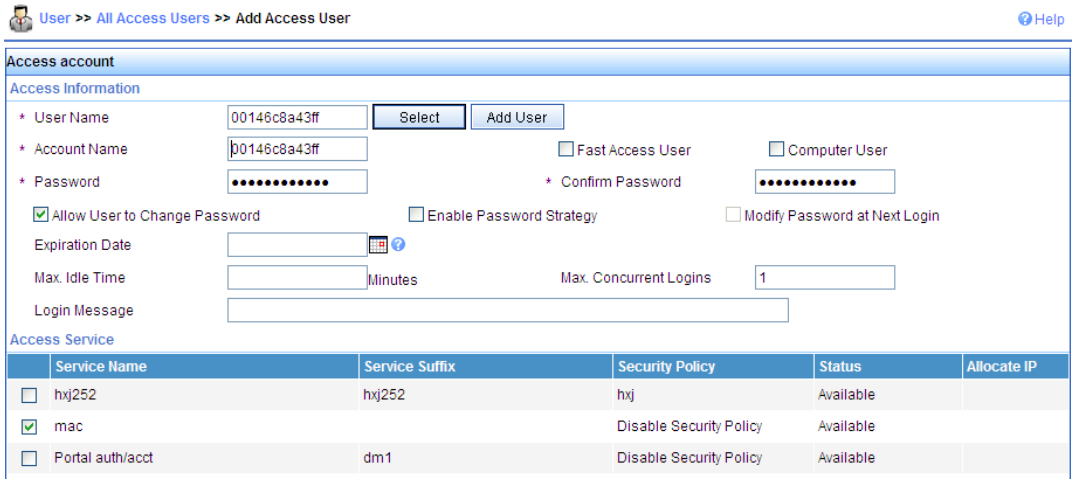
2. Add a service:
   a. Click the **Service** tab.
   b. Select **User Access Manager** > **Service Configuration** from the navigation tree.
   c. Click **Add**.
   d. On the page that appears, set the service name to **mac**, keep the default values for other parameters, and click **Apply**.

Figure 19 Adding a service



3. Add an account:
   a. Click the **User** tab.
   b. Select **User** > **All Access Users** from the navigation tree to enter the user page.
   c. Click **Add**.
   d. On the page that appears, enter username **00146c8a43ff**, set the account name and password both to **00146c8a43ff**, select the service **mac**, and click **Apply**.

Figure 20 Adding an account



Verifying the configuration

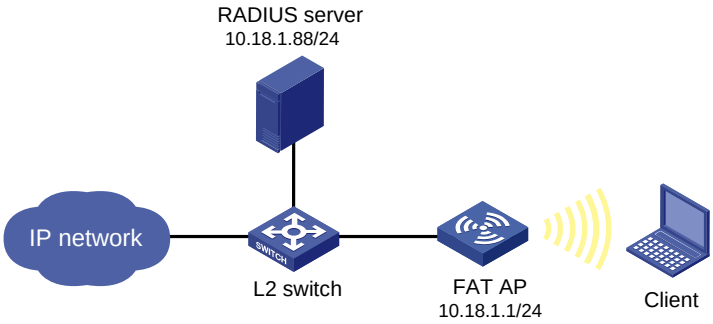
- After the client passes the MAC address authentication, the client can associate with the AP and access the WLAN.
- You can use the **display wlan client** command, the **display connection** command, and the **display mac-authentication** command to view the online clients.

802.1X authentication configuration example

Network requirements

As shown in Figure 21, configure the FAT AP to perform 802.1X authentication on the client.

Figure 21 Network diagram



Configuration procedure

1. Configure the fat AP:

   # Enable port security.

   ```
   <Sysname> system-view
   [Sysname] port-security enable
   ```

   # Configure the 802.1X authentication mode as **EAP**.

   ```
   [Sysname] dot1x authentication-method eap
   ```

   # Create a RADIUS scheme **rad**, and specify the extended RADIUS server type.

   ```
   [Sysname] radius scheme rad
   [Sysname-radius-rad] server-type extended
   ```

   # Configure the IP addresses of the primary authentication server and accounting server as 10.18.1.88.

   ```
   [Sysname-radius-rad] primary authentication 10.18.1.88
   [Sysname-radius-rad] primary accounting 10.18.1.88
   ```

   # Configure the shared key for RADIUS authentication/accounting packets as **12345678**.

   ```
   [Sysname-radius-rad] key authentication 12345678
   [Sysname-radius-rad] key accounting 12345678
   [Sysname-radius-rad] user-name-format without-domain
   [Sysname-radius-radius1] quit
   ```

   # Configure AAA domain **cams** by referencing RADIUS scheme **rad**.

   ```
   [Sysname] domain cams
   [Sysname-isp-cams] authentication lan-access radius-scheme rad
   [Sysname-isp-cams] authorization lan-access radius-scheme rad
   [Sysname-isp-cams] accounting lan-access radius-scheme rad
   [Sysname-isp-cams] quit
   ```

   # Specify **cams** as the default ISP domain.

   ```
   [Sysname] domain default enable cams
   ```

   # Configure the port security mode as **userlogin-secure-ext**, and enable 802.11 key negotiation on the interface WLAN-BSS 1.

   ```
   [Sysname] interface wlan-bss 1
   [Sysname-WLAN-BSS1] port-security port-mode userlogin-secure-ext
   [Sysname-WLAN-BSS1] port-security tx-key-type 11key
   ```

   # Disable the multicast trigger function and the online user handshake function.

   ```
   [Sysname-WLAN-BSS1] undo dot1x multicast-trigger
   [Sysname-WLAN-BSS1] undo dot1x handshake
   [Sysname-WLAN-BSS1] quit
   ```

Create crypto-type service template 1, configure its SSID as dot1x, and configure the tkip and ccmp cipher suite.

```
[Sysname] wlan service-template 1 crypto
[Sysname-wlan-st-1] ssid dot1x
```

Enable the RSN-IE in the beacon and probe responses and enable the AES-CCMP cipher suite in the encryption of frames.

```
[Sysname-wlan-st-1] authentication-method open-system
[Sysname-wlan-st-1] cipher-suite ccmp
[Sysname-wlan-st-1] security-ie rsn
[Sysname-wlan-st-1] service-template enable
[Sysname-wlan-st-1] quit
```

On interface WLAN-radio 2/0, bind service template 1 to interface WLAN-BSS 1.

```
[Sysname] interface wlan-radio2/0
[Sysname-WLAN-Radio2/0] radio-type dot11g
[Sysname-WLAN-Radio2/0] service-template 1 interface wlan-bss 1
```

2. Configure the RADIUS server (IMCv3):

   See "Configuring the RADIUS server (IMCv3)."

3. Configure the RADIUS server (IMCv5):

   See "Configuring the RADIUS server (IMCv5)."

4. Configure the wireless card:

   a. Double click the  icon at the bottom right corner of your desktop.

      The **Wireless Network Connection Status** window appears.

   b. Click the **Properties** button in the **General** tab.

      The **Wireless Network Connection Properties** window appears.

   c. In the **Wireless Networks** tab, select the wireless network with the SSID **dot1x**, and then click **Properties**.

      The **dot1x Properties** window appears. See Figure 22.

   d. In the **Authentication** tab, select **Protected EAP (PEAP)** from the **EAP type** list, and click **Properties**.

   e. In the popup window, clear **Validate server certificate**, and click **Configure**. See Figure 23.

   f. In the popup dialog box, clear **Automatically use my Windows logon name and password (and domain if any)**. See Figure 24.

Figure 22 Configuring the wireless card (1)

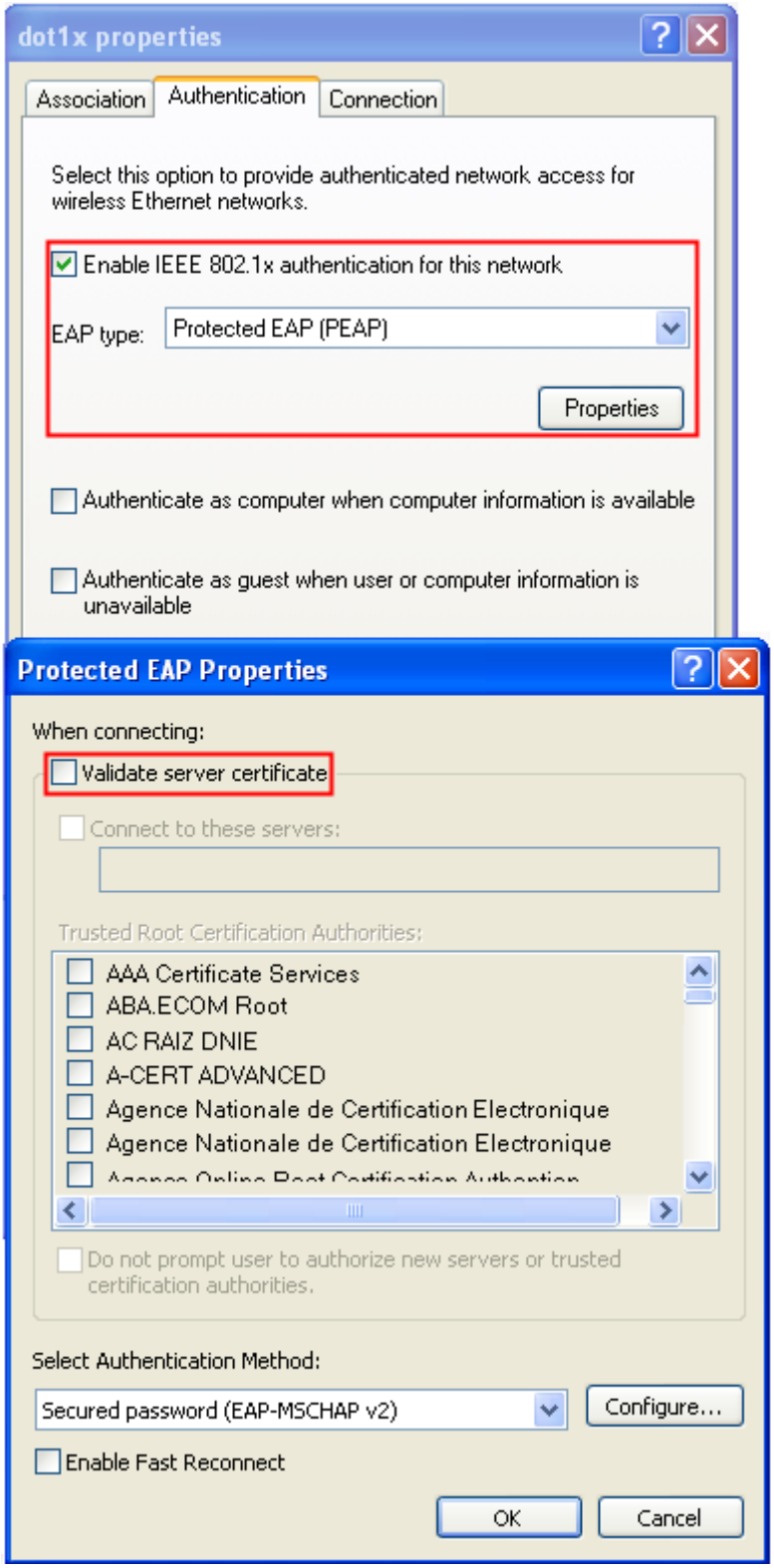


Figure 23 Configuring the wireless card (2)

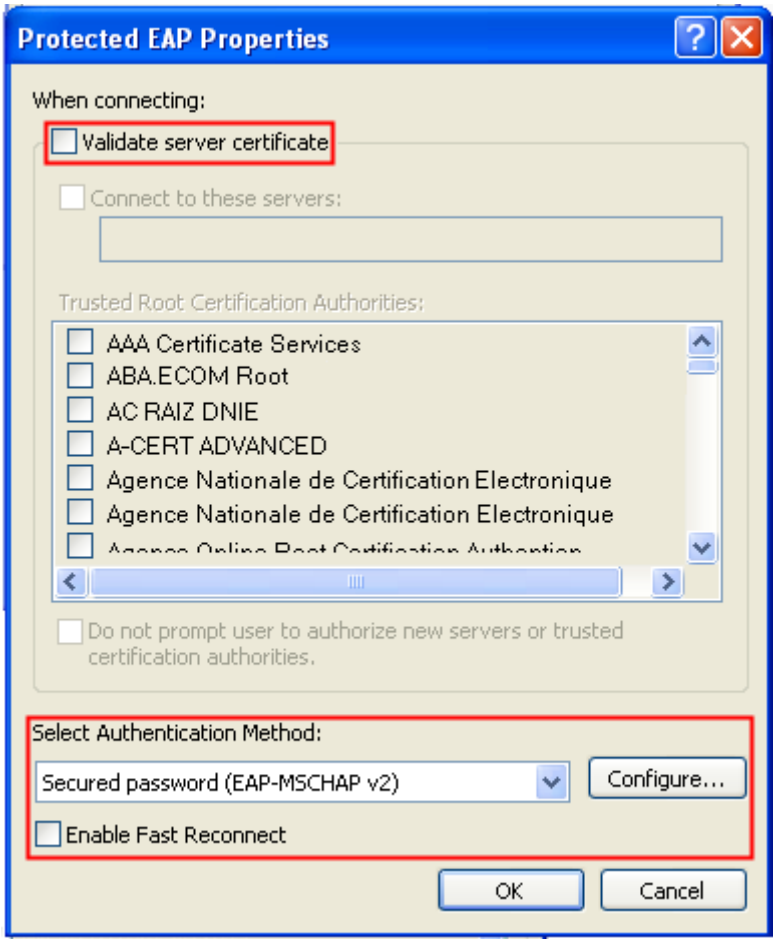
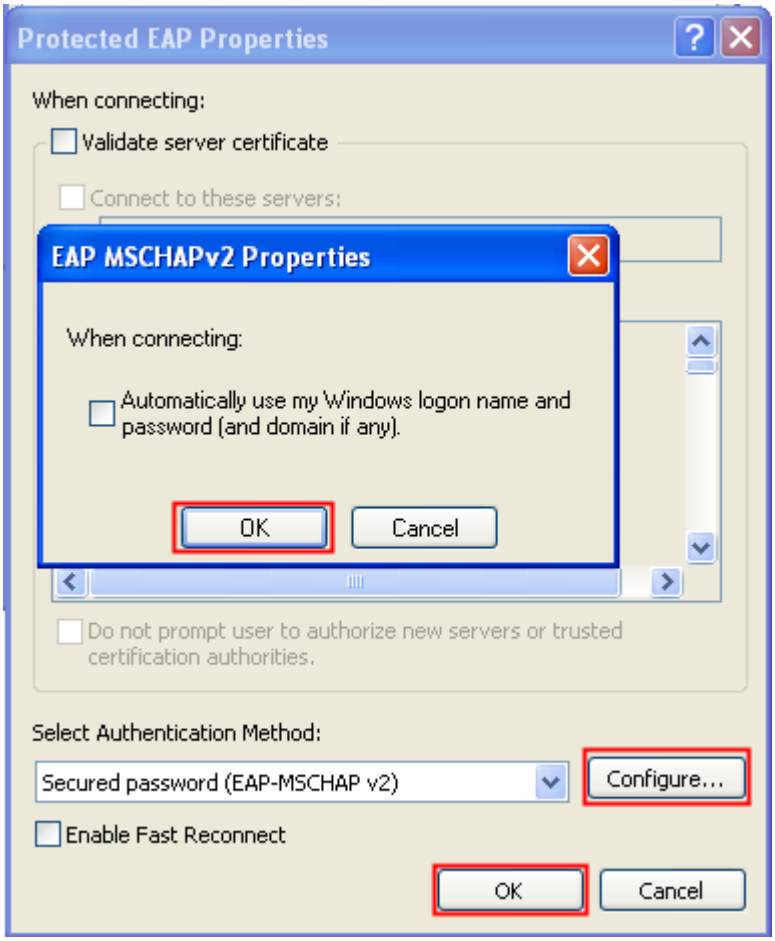


Figure 24 Configuring the wireless card (3)



Verifying the configuration.

- Enter the username **user** and password **dot1x**. The client can pass 802.1X authentication and access the WLAN.
- You can use the **display wlan client** command, **display connection** command and **display dot1x** command to view the online clients.

Supported combinations for ciphers

This section introduces the combinations that can be used during the cipher suite configuration.

RSN

For RSN, the WLAN-WSEC module supports only AES-CCMP and TKIP ciphers as the pair wise ciphers and WEP cipher suites are only used as group cipher suites. Below are the cipher suite combinations that WLAN-WSEC supports for RSN. (WEP40, WEP104 and WEP128 are mutually exclusive).

Unicast cipher	Broadcast cipher	Authentication method	Security Type
CCMP	WEP40	PSK	RSN
CCMP	WEP104	PSK	RSN
CCMP	WEP128	PSK	RSN

Unicast cipher	Broadcast cipher	Authentication method	Security Type
CCMP	TKIP	PSK	RSN
CCMP	CCMP	PSK	RSN
TKIP	WEP40	PSK	RSN
TKIP	WEP104	PSK	RSN
TKIP	WEP128	PSK	RSN
TKIP	TKIP	PSK	RSN
CCMP	WEP40	802.1X	RSN
CCMP	WEP104	802.1X	RSN
CCMP	WEP128	802.1X	RSN
CCMP	TKIP	802.1X	RSN
CCMP	CCMP	802.1X	RSN
TKIP	WEP40	802.1X	RSN
TKIP	WEP104	802.1X	RSN
TKIP	WEP128	802.1X	RSN
TKIP	TKIP	802.1X	RSN

WPA

For WPA, the WLAN-WSEC module supports the CCMP and TKIP ciphers as the pair wise ciphers and WEP cipher suites are only used as group cipher suites. Below are the cipher suite combinations that WLAN-WSEC supports for WPA (WEP40, WEP104 and WEP128 are mutually exclusive).

Unicast cipher	Broadcast cipher	Authentication method	Security Type
CCMP	WEP40	PSK	WPA
CCMP	WEP104	PSK	WPA
CCMP	WEP128	PSK	WPA
CCMP	TKIP	PSK	WPA
CCMP	CCMP	PSK	WPA
TKIP	WEP40	PSK	WPA
TKIP	WEP104	PSK	WPA
TKIP	WEP128	PSK	WPA
TKIP	TKIP	PSK	WPA
CCMP	WEP40	802.1X	WPA
CCMP	WEP104	802.1X	WPA
CCMP	WEP128	802.1X	WPA
CCMP	TKIP	802.1X	WPA
CCMP	CCMP	802.1X	WPA
TKIP	WEP40	802.1X	WPA
TKIP	WEP104	802.1X	WPA

Unicast cipher	Broadcast cipher	Authentication method	Security Type
TKIP	WEP128	802.1X	WPA
TKIP	TKIP	802.1X	WPA

Pre-RSN

For Pre-RSN stations, the WLAN-WSEC module supports only WEP cipher suites. (WEP40, WEP104 and WEP128 are mutually exclusive).

Unicast cipher	Broadcast cipher	Authentication method	Security Type
WEP40	WEP40	Open system	no Sec Type
WEP104	WEP104	Open system	no Sec Type
WEP128	WEP128	Open system	no Sec Type
WEP40	WEP40	Shared key	no Sec Type
WEP104	WEP104	Shared key	no Sec Type
WEP128	WEP128	Shared key	no Sec Type

Configuring WLAN IDS

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.

Overview

802.11 networks are susceptible to a wide array of threats such as unauthorized access points and clients, ad hoc networks, and DoS attacks. Rogue devices are a serious threat to enterprise security. Wireless intrusion detection system (WIDS) is used for the early detection of malicious attacks and intrusions on a wireless network. WIPS helps to protect enterprise networks and users from unauthorized wireless access. The Rogue detection feature is a part of the WIDS/WIPS solution, which detects the presence of rogue devices in a WLAN network and takes countermeasures to prevent rogue devices operation.

Terminology

- **WIDS**—WLAN IDS is designed to be deployed in an area that an existing wireless network covers. It aids in the detection of malicious outsider attacks and intrusions through the wireless network.
- **Rogue AP**—An unauthorized or malicious access point on the network, such as an employee setup AP, misconfigured AP, neighbor AP or an attacker operated AP. It is not authorized, so if any vulnerability occurs on the AP, the hacker has a chance to compromise your network security.
- **Rogue client**—An unauthorized or malicious client on the network.
- **Rogue wireless bridge**—Unauthorized wireless bridge on the network.
- **Monitor AP**—An AP that scans or listens to 802.11 frames to detect wireless attacks in the network.
- **Ad hoc mode**—Sets the working mode of a wireless client to ad hoc. An ad hoc terminal can communicate directly with other stations without support from any other device.
- **Passive scanning**—In passive scanning, a monitor AP listens to all the 802.11 frames over the air in that channel.
- **Active scanning**—In active scanning, a monitor AP, besides listening to all 802.11 frames, sends a broadcast probe request and receives all probe response messages on that channel. Each AP in the vicinity of the monitor AP replies to the probe request. This helps identify all authorized and unauthorized APs by processing probe response frames. The monitor AP masquerades as a client when sending the probe request.

Attack detection

The attack detection function detects intrusions or attacks on a WLAN network, and informs the network administrator of the attacks through recording information or sending logs. At present, WIDS detection supports detection of the following attacks:

- Flood attack
- Spoofing attack
- Weak IV attack

Flood attack detection

A flood attack refers to the case where WLAN devices receive large volumes of frames of the same kind within a short span of time. When this occurs, the WLAN devices are overwhelmed. Consequently, they are unable to service normal clients.

WIDS attacks detection counters flood attacks by constantly keeping track of the density of traffic generated by each device. When the traffic density of a device exceeds the limit, the device is considered flooding the network and, if the dynamic blacklist feature is enabled, is added to the blacklist and forbidden to access the WLAN for a period of time.

WIDS inspects the following types of frames:

- Authentication requests and de-authentication requests
- Association requests, disassociation requests and reassociation requests
- Probe requests
- 802.11 null data frames
- 802.11 action frames.

Spoofing attack detection

In this kind of attack, a potential attacker can send frames in the air on behalf of another device. For instance, a client in a WLAN has been associated with an AP and operates correctly. In this case, a spoofed de-authentication frame can cause a client to get de-authenticated from the network and can affect the normal operation of the WLAN.

At present, spoofing attack detection counters this type of attack by detecting broadcast de-authentication and disassociation frames sent on behalf of an AP. When such a frame is received, it is identified as a spoofed frame, and the attack is immediately logged.

Weak IV detection

WEP uses an IV to encrypt each frame. An IV and a key are used to generate a key stream, and thus encryptions using the same key have different results. When a WEP frame is sent, the IV used in encrypting the frame is also sent as part of the frame header.

However, if a WLAN device generates IVs in an insecure way, for example, if it uses a fixed IV for all frames, the shared secret key might be exposed to any potential attackers. When the shared secret key is compromised, the attacker can access network resources.

Weak IV detection counters this attack by verifying the IVs in WEP frames. Whenever a frame with a weak IV is detected, it is immediately logged.

Blacklist and white list

You can configure the blacklist and white list functions to filter frames from WLAN clients and implement client access control.

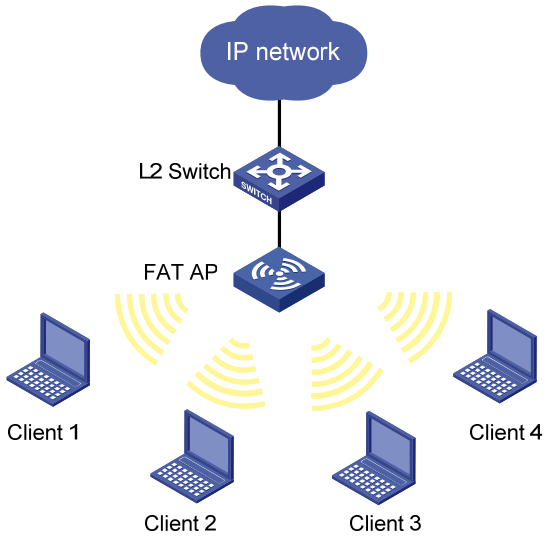
WLAN client access control is accomplished through the following types of lists.

- **White list**—Contains the MAC addresses of all clients allowed to access the WLAN. If the white list is used, only permitted clients can access the WLAN, and all frames from other clients are discarded.
- **Static blacklist**—Contains the MAC addresses of clients forbidden to access the WLAN. This list is manually configured.
- **Dynamic blacklist**—Contains the MAC addresses of clients forbidden to access the WLAN. A client is dynamically added to the list if it is considered sending attacking frames until the timer of the entry expires.

When an AP receives an 802.11 frame, it checks the source MAC address of the frame and processes the frame by following these rules:

1. If the source MAC address does not match any entry in the white list, the frame is dropped. If there is a match, the frame is considered valid and is processed further.
2. If no white list entries exist, the static and dynamic blacklists are searched.
3. If the source MAC address matches an entry in any of the two lists, the frame is dropped.
4. If there is no match, or no blacklist entries exist, the frame is considered valid and is processed further.

Figure 25 Frame filtering



If client 1 is present in the backlist, it cannot associate with the fat AP. If it is only in the white list, it can get associated with the fat AP.

Hardware compatibility with WLAN

WLAN IDS is not available on the following routers:

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

WLAN IDS configuration task list

Task		Description
Configuring AP operating mode		Required.
Configuring attack detection	Configuring attack detection.	Optional.
	Displaying and maintaining attack detection.	
Configuring blacklist and whitelist		Optional.

Configuring AP operating mode

A WLAN consists of various APs that span across the building offering WLAN services to the clients. The administrator may want some of these APs to detect rogue devices. The administrator can configure an AP to operate in any of the three modes, normal, monitor, or hybrid.

- In normal mode, an AP provides WLAN data services but does not perform any scanning.
- In monitor mode, an AP scans all Dot11 frames in the WLAN, but cannot provide WLAN services. An AP operating in this mode cannot provide WLAN service, and you do not need to configure a service template.
- In hybrid mode, an AP can both scan devices in the WLAN and provide WLAN services. For an AP operating in this mode, you need to configure a service template so that the AP can provide WLAN service when scanning devices.

To configure the AP operating mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the AP operating mode.	• Configure the AP operating mode as monitor: **wlan work-mode monitor** • Configure the AP operating mode as hybrid: **wlan device-detection enable**	Use either command. By default, the AP operating mode is **normal**. • When an AP has its operating mode changed from normal to monitor, it does not restart. • When an AP has its operating mode changed from monitor to normal, it restarts.

Configuring attack detection

Configuring attack detection

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IDS view.	**wlan ids**	N/A
3. Enable IDS attack detection.	**attack-detection enable** { **all** | **flood** | **spoof** | **weak-iv** }	By default, IDS attack detection is disabled.

Displaying and maintaining attack detection

Task	Command	Remarks
Display all the attacks detected by WLAN IDS IPS.	**display wlan ids history** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the count of attacks detected by WLAN IDS IPS.	**display wlan ids statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

Task	Command	Remarks
Clear the history of attacks detected by the WLAN system.	**reset wlan ids history**	Available in user view.
Clear the statistics of attacks detected in the WLAN system.	**reset wlan ids statistics**	Available in user view.

Configuring blacklist and whitelist

Perform this task to configure the static blacklist, static white list, enable dynamic blacklist feature, and configure the lifetime for dynamic entries.

- WLAN IDS permits devices present in the static white list. You can add entries into or delete entries from the list.
- WLAN IDS denies devices present in the static blacklist. You can add entries into or delete entries from the list.
- WLAN IDS adds dynamically detected attack devices into the dynamic blacklist. You can set a lifetime in seconds for dynamic blacklist entries. After the lifetime of an entry expires, the device entry will be removed from the dynamic blacklist. If a flood attack from the device is detected again before the lifetime expires, the entry is refreshed.

Configuring static lists

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN IDS view.	**wlan ids**	N/A
3. Add an entry into the white list.	**whitelist mac-address** *mac-address*	Optional. By default, no white list exists.
4. Add an entry into the static blacklist.	**static-blacklist mac-address** *mac-address*	Optional. By default, no static blacklist exists.

Configuring dynamic blacklist

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN IDS view.	**wlan ids**	N/A
3. Enable the dynamic blacklist feature.	**dynamic-blacklist enable**	Optional. By default, the dynamic blacklist feature is disabled.
4. Configure the lifetime for dynamic blacklist entries.	**dynamic-blacklist lifetime** *lifetime*	Optional. By default, the lifetime is 300 seconds.

Displaying and maintaining blacklist and whitelist

Task	Command	Remarks
Display blacklist entries.	**display wlan blacklist** { **static** | **dynamic** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display white list entries.	**display wlan whitelist** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Clear dynamic blacklist entries.	**reset wlan dynamic-blacklist** { **mac-address** *mac-address* | **all** }	Available in user view.

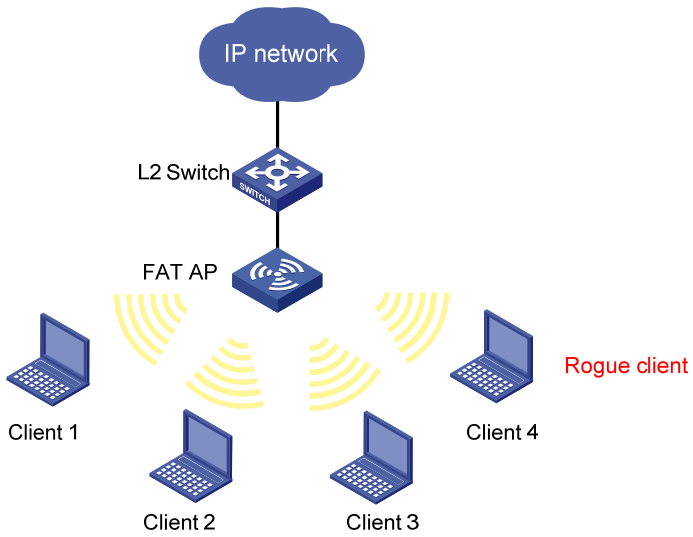
WLAN IDS configuration examples

WLAN IDS configuration example

Network requirements

As shown in Figure 26, WLAN IDS allows Client 1 (MAC address 000f-e215-1515), Client 2 (MAC address 000f-e215-1530) and Client 3 (MAC address 000f-e213-1235) to access the fat AP. Configure the operating mode of the fat AP as hybrid to enable it to provide WLAN access services and detect rogue clients in the network.

Figure 26 Network diagram



Configuration procedure

Create a WLAN ESS interface.

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

Create service template 1 of clear type, configure its SSID as **service**.

```
[AP] wlan service-template 1 clear
```

```
[AP-wlan-st-1] ssid service
[AP-wlan-st-1] authentication-method open-system
[AP-wlan-st-1] service-template enable
[AP-wlan-st-1] quit
```

Bind WLAN-Radio 2/0 to service template 1 and WLAN-BSS 1.

```
[AP] interface Wlan-radio 2/0
[AP-Wlan-radio2/0] service-template 1 interface WLAN-BSS 1
[AP-Wlan-radio2/0] quit
```

Configure the AP to operate in hybrid mode. It scans rogue devices and provides access services.

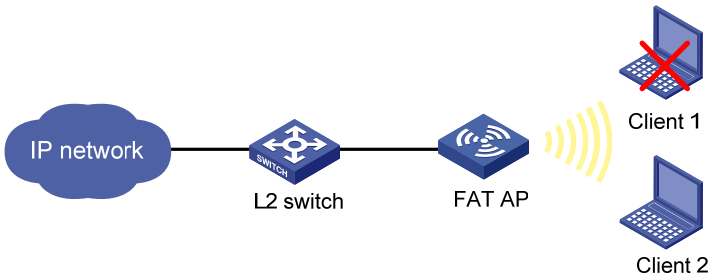
```
[AP] wlan device-detection enable
```

Blacklist and whitelist configuration example

Network requirements

As shown in Figure 27, to ensure WLAN security, add the MAC address of the client into the blacklist on the AC to disable it from accessing the wireless network through any AP.

Figure 27 Network diagram



Configuration procedure

Add MAC address **0000-000f-1211** of Client 1 into the blacklist.

```
<Sysname> system-view
[Sysname] wlan ids
[Sysname-wlan-ids] static-blacklist mac-address 0000-000f-1211
```

After the configuration, Client 1 cannot access the AP, and other clients can access the network.

Configuring WLAN QoS

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.

Overview

An 802.11 network offers contention-based wireless access. To provide applications with QoS services, IEEE developed 802.11e for the 802.11-based WLAN architecture.

While IEEE 802.11e was being standardized, Wi-Fi Alliance defined the Wi-Fi Multimedia (WMM) standard to allow QoS provision devices of different vendors to interoperate. WMM makes a WLAN network capable of providing QoS services.

Terminology

- **WMM**—A wireless QoS protocol designed to preferentially transmit packets with high priority, thus guaranteeing better QoS services for voice and video applications in a wireless network.
- **Enhanced distributed channel access (EDCA)**—A channel contention mechanism designed by WMM to preferentially transmit packets with high priority and allocate more bandwidth to such packets.
- **Access category (AC)**—Used for channel contention. WMM defines four access categories; they are AC-VO (voice) queue, AC-VI (video) queue, AC-BE (best-effort) queue, and AC-BK (background) queue in the descending order of priority. When contending for a channel, a high-priority AC queue preempts a low-priority AC queue.
- **Connection admission control (CAC)**—Limits the number of clients that are using high-priority AC queues (including AC-VO and AC-VI queues) to guarantee sufficient bandwidth for existing high-priority traffic.
- **Unscheduled Automatic Power-Save Delivery (U-APSD)**—A new power saving mechanism defined by WMM to enhance the power saving capability of clients.
- **SpectraLink voice priority (SVP)**—A voice priority protocol designed by the SpectraLink company to guarantee QoS for voice traffic.

WMM protocol

The distributed coordination function (DCF) in 802.11 stipulates that access points (APs) and clients use the carrier sense multiple access with collision avoidance (CSMA/CA) access mechanism. APs or clients listen to the channel before they hold the channel for data transmission. When the specified idle duration of the channel times out, APs or clients randomly select a backoff slot within the contention window to perform backoff. The device that finishes backoff first gets the channel. With 802.11, all devices have the same idle duration and contention window. Therefore, they are equal when contending for a channel. In WMM, this fair contention mechanism is changed.

EDCA parameters

WMM assigns data packets in a basic service set (BSS) to four AC queues. By allowing a high-priority AC queue to have more channel contention opportunities than a low-priority AC queue, WMM offers different service levels to different AC queues.

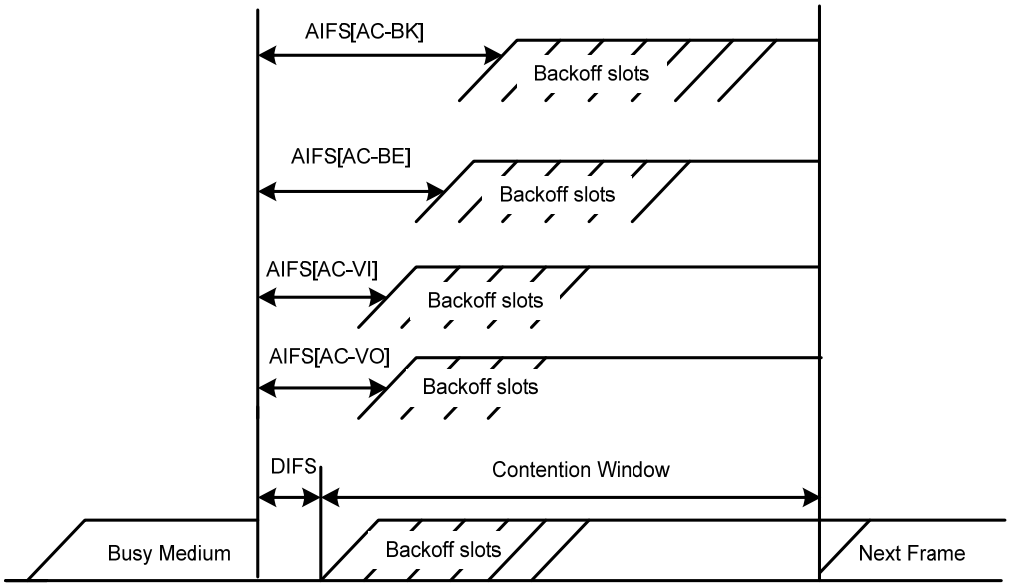
WMM define a set of EDCA parameters for each AC queue, covering the following:

- **Arbitration inter-frame spacing number (AIFSN)**—Different from the 802.11 protocol where the idle duration (set using DIFS) is a constant value, WMM can define an idle duration per AC

queue. The idle duration increases as the AIFSN value increases (see Figure 28 for the AIFS durations).

- **Exponent form of CWmin (ECWmin) and exponent form of CWmax (ECWmax)**—Determine the average backoff slots, which increases as the two values increase (see Figure 28 for the backoff slots).
- **Transmission opportunity limit (TXOPLimit)**—Indicates the maximum time for which a user can hold a channel after a successful contention. The greater the TXOPLimit is, the longer the user can hold the channel. The value 0 indicates that the user can send only one packet each time it holds the channel.

Figure 28 Per-AC channel contention parameters in WMM



CAC admission policies

CAC requires that a client obtain permission of the AP before it can use a high-priority AC queue for transmission, guaranteeing bandwidth to the clients that have gained access. CAC controls real time traffic (AC-VO and AC-VI traffic) but not common data traffic (AC-BE and AC-BK traffic).

If a client wants to use a high-priority AC queue, it must send a request to the AP. The AP returns a positive or negative response based on either of the following admission control policies:

- **Channel utilization-based admission policy**—The AP calculates the total time that the existing high-priority AC queues occupy the channel in one second, and then calculates the time that the requesting traffic will occupy the channel in one second. If the sum of the two values is smaller than or equal to the maximum hold time of the channel, the client can use the requested AC queue. Otherwise, the request is rejected.
- **Users-based admission policy**—If the number of clients using high-priority AC queues plus the clients requesting for high-priority AC queues is smaller than or equal to the maximum number of high-priority AC queue clients, the request is accepted. Otherwise, the request is rejected. During calculation, a client is counted once even if it is using both the AC-VO and AC-VI queues.

U-APSD power-save mechanism

U-APSD improves the 802.11 APSD power saving mechanism. When associating clients with AC queues, you can specify some AC queues as trigger-enabled, some AC queues as delivery-enabled, and the maximum number of data packets that can be delivered after receiving a trigger packet. Both the trigger attribute and the delivery attribute can be modified when flows are established using CAC. When a client sleeps, the delivery-enabled AC queue packets destined for the client are buffered. The client must send a trigger-enabled AC queue packet to get the buffered packets. After the AP

receives the trigger packet, packets in the transmit queue are sent. The number of sent packets depends on the agreement made when the client was admitted. AC queues without the delivery attribute store and transmit packets as defined in the 802.11 protocol.

SVP

SVP can assign packets with the protocol ID 119 in the IP header to a specific AC queue. SVP stipulates that random backoff is not performed for SVP packets. Therefore, you can set both ECWmin and ECWmax to 0 when there are only SVP packets in an AC queue.

ACK policy

WMM defines two ACK policies:

- **No ACK**—When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.
- **Normal ACK**—When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

Protocols and standards

- 802.11e-2005, Amendment 8: *Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society, 2005*
- *Wi-Fi, WMM Specification version 1.1, Wi-Fi Alliance, 2005*

Hardware compatibility with WLAN

WLAN is not available on the following routers:

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

Configuring WMM

Configuration restrictions and guidelines

- If CAC is enabled for an AC queue, CAC is also enabled for the 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.
- H3C recommends that you use the default EDCA parameter settings for APs and clients (except the TXOPLimit parameter for devices using 802.11b radio cards) unless it is necessary to modify the default settings.
- When the radio card of a device is 802.11b, H3C recommends that you set the TXOPLimit values of the AC-BK, AC-BE, AC-VI, and AC-VO queues to 0, 0, 188, and 102, respectively.
- The SVP packet mapping function takes effect only after you enable WMM.

Configuration procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter WLAN-radio interface view.	**interface wlan-radio** *radio-number*	N/A
3. Enable WMM.	**wmm enable**	By default, WMM is enabled. The 802.11n protocol stipulates that all 802.11n clients support WLAN QoS. Therefore, when the radio operates in 802.11gn mode, you should enable WMM. Otherwise, the associated 802.11n clients might fail to communicate.
4. Set the EDCA parameters of AC-VO or AC-VI queues for clients.	**wmm edca client** { **ac-vo** | **ac-vi** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax -value* | **txoplimit** *txoplimit-value* | **cac** } *	Optional. By default, a client uses the default EDCA parameters shown in Table 3.
5. Set the EDCA parameters of AC-BE or AC-BK queues for clients.	**wmm edca client** { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax -value* | **txoplimit** *txoplimit -value* } *	Optional. By default, a client uses the default EDCA parameters shown in Table 3.
6. Set the EDCA parameters and specify the ACK policy for the radio.	**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** } *	Optional. By default, an AP uses the default EDCA parameters shown in Table 4 and uses the Normal ACK policy.
7. Set the CAC policy.	**wmm cac policy** { **channelutilization** [*channelutilization-value*] | **users** [*users-number*] }	Optional. By default, the users-based admission policy applies, with the maximum number of users being 20.
8. Map SVP packets to a specified AC queue.	**wmm svp map-ac** { **ac-vi** | **ac-vo** | **ac-be** | **ac-bk** }	Optional. By default, the SVP packet mapping function is disabled. SVP packet mapping applies to non WMM clients, and does not take effect on WMM clients.

Table 3 The default EDCA parameters for clients

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

Table 4 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

Displaying and maintaining WMM

Task	Command	Remarks
Display WLAN statistics of the specified client.	**display wlan statistics client** { **all** | **mac-address** *mac-address* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display WMM configuration information of the specified radio or client.	**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*]	Available in any view.
Clear WMM statistics of the specified radio or client.	**reset wlan wmm** { **radio** [**interface wlan-radio** *wlan-radio-number*] | **client** { **all | interface wlan-radio** *wlan-radio-number* | **mac-address** *mac-address* } }	Available in any view.

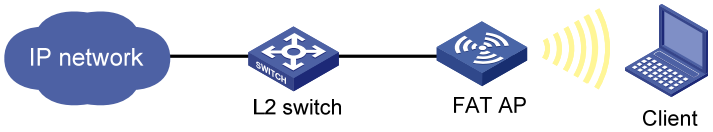
WMM configuration examples

WMM basic configuration example

1. Network requirements

   As shown in Figure 29, enable WMM on the fat AP, so that the fat AP and client can prioritize the traffic.

   Figure 29 Network diagram

2. Configuration procedure

   # Configure interface WLAN-BSS 1 to use the 802.11e priority of the received packets for priority mapping.

   ```
   <Sysname> system-view
   [Sysname] interface wlan-bss 1
   [Sysname-WLAN-BSS1] qos trust dot11e
   ```

```
[Sysname-WLAN-BSS1] quit
```

Configure interface Ethernet 1/0 to use the 802.1p priority of received packets for priority mapping.

```
[Sysname] interface Ethernet 1/0
[Sysname-Ethernet1/0] qos trust dot1p
[Sysname-Ethernet1/0] quit
```

Create a clear-type WLAN service template, configure its SSID as **market**, configure its authentication method as Open System, and then enable the WLAN service template.

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

Configure the radio type as 802.11g for radio interface WLAN-Radio 2/0, and map service template 1 to interface WLAN-BSS1 on the radio interface.

```
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] radio-type dot11g
[Sysname-WLAN-Radio2/0] service-template 1 interface wlan-bss 1
```

Enable WMM on radio interface WLAN-Radio 2/0/.

```
[Sysname-WLAN-Radio2/0] wmm enable
[Sysname-WLAN-Radio2/0] quit
```

After WMM is enabled, you can use the **display wlan wmm radio** command to view WMM-related information.

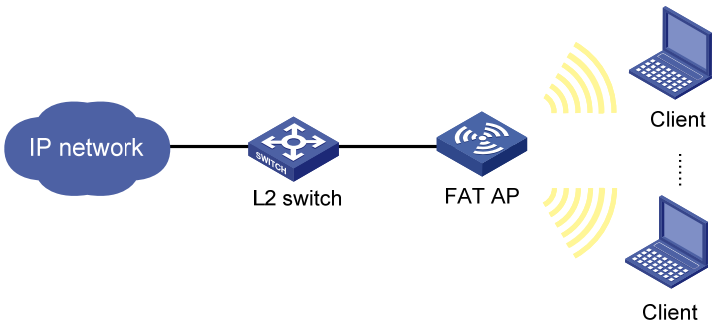
CAC service configuration example

1. Network requirements

   As shown in Figure 30, a fat AP is connected to an Ethernet and has WMM enabled.

   Enable CAC for the AC-VO and AC-VI queues of the fat AP. Use a users-based admission policy to allow up to 10 users to access, so that enough bandwidth can be guaranteed for the clients using high-priority queues (AC-VO and AC-VI queues).

   Figure 30 Network diagram



2. Configuration procedure

   # Configure interface WLAN-BSS 1 to use the 802.11e priority of received packets for priority mapping.

```
<Sysname> system-view
[Sysname] interface wlan-bss 1
[Sysname-WLAN-BSS1] qos trust dot11e
[Sysname-WLAN-BSS1] quit
```

   # Configure interface Ethernet 1/0 to use the 802.1p priority of received packets for priority mapping.

```
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] qos trust dot1p
[Sysname-Ethernet1/0] quit
```

Create a clear-type WLAN service template, configure its SSID as **market**, configure its authentication method as Open System, and then enable the WLAN service template.

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

Configure the radio type as 802.11g for radio interface WLAN-Radio 2/0, and map service template 1 to interface WLAN-BSS1 on the radio interface.

```
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] radio-type dot11g
[Sysname-WLAN-Radio2/0] service-template 1 interface wlan-bss 1
```

Configure radio interface WLAN-radio 2/0 to allow up to ten users to use high-priority AC queues (including AC-VO and AC-VI queues).

```
[Sysname-WLAN-Radio2/0] wmm edca client ac-vo cac
[Sysname-WLAN-Radio2/0] wmm edca client ac-vi cac
[Sysname-WLAN-Radio2/0] wmm cac policy users 10
[Sysname-WLAN-Radio2/0] wmm enable
[Sysname-WLAN-Radio2/0] quit
```

If a client wants to use a high-priority AC queue (AC-VO or AC-VI queue), it must send a request to the AP. If the number of clients using high-priority AC queues (including AC-VO and AC-VI queues) plus the clients requesting for high-priority AC queues on the AP is smaller than or equal to the maximum number of high-priority AC clients (10 in this example), the request is accepted. If the number of client exceeds the maximum number of high-priority AC clients, the system decreases the priority of the packets from the excessive clients.

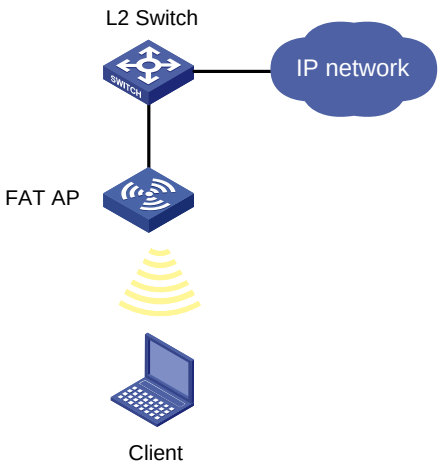
SVP service configuration example

1. Network requirements

   As shown in Figure 31, the fat AP is connected to the Ethernet and has WMM enabled.

   On the fat AP, SVP packets are assigned to the AC-VO queue. To guarantee the highest priority for the AC-VO queue, ECWmin and ECWmax are set to 0 for the AC-VO queue.

   Figure 31 Network diagram



2. Configuration procedure

Configure interface WLAN-BSS 1 to use the 802.11e priority of received packets for priority mapping.

```
<Sysname> system-view
[Sysname] interface wlan-bss 1
[Sysname-WLAN-BSS1] qos trust dot11e
[Sysname-WLAN-BSS1] quit
```

Configure interface Ethernet 1/0 to use the 802.1p priority of received packets for priority mapping.

```
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] qos trust dot1p
[Sysname-Ethernet1/0] quit
```

Create a clear-type WLAN service template, configure its SSID as **market**, configure its authentication method as Open System, and then enable the WLAN service template.

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

Configure the radio interface WLAN Radio 2/0.

```
[Sysname] interface wlan-radio 2/0
[Sysname-WLAN-Radio2/0] radio-type dot11g
[Sysname-WLAN-Radio2/0] service-template 1 interface wlan-bss 1
[Sysname-WLAN-Radio2/0] wmm enable
[Sysname-WLAN-Radio2/0] wmm svp map-ac ac-vo
[Sysname-WLAN-Radio2/0] wmm edca radio ac-vo ecw ecwmin 0 ecwmax 0
[Sysname-WLAN-Radio2/0] quit
```

If a non-WMM client goes online and sends SVP packets to the AP, the SVP packets are assigned to the AC-VO queue.

Troubleshooting

EDCA parameter configuration failure

Symptom

Configuring EDCA parameters for an AP failed.

Analysis

The EDCA parameter configuration of an AP is restricted by the radio chip of the AP.

Solution

1. Use the **display wlan wmm radio ap** command to view the support of the radio chip for the EDCA parameters. Make sure the configured EDCA parameters are supported by the radio chip.
2. Check that the values configured for the EDCA parameters are valid.
3. Make sure the client is a non-WMM client, because SVP takes effect on only non-WMM clients.

SVP or CAC configuration failure

Symptom

The SVP packet priority mapping function configured with the **wmm svp map-ac** command does not take effect.

CAC configured with the **wmm edca client** command does not take effect.

Analysis

The SVP packet priority mapping function or CAC takes effect only after WMM is enabled.

Solution

1. Use the **wmm enable** command to enable the WMM function.
2. Check the state of the SVP priority mapping function or CAC again.
3. The SVP packet priority mapping function takes effect on only non-WMM clients. Check whether the client is a non-WMM client.

Configuring client rate limiting

The WLAN provides limited bandwidth for each AP. Because the bandwidth is shared by wireless clients attached to the AP, aggressive use of bandwidth by a client will affect other clients. To ensure fair use of bandwidth, rate limit traffic of clients in either of the following methods:

- Configure the total bandwidth shared by all clients. This is called "dynamic mode." The rate limit of a client is the configured total rate/the number of online clients. For example, if the configure total rate is 10 Mbps and five clients are online, the rate limit of each client is 2 Mbps.
- Configure the maximum bandwidth that can be used by each client. This is called "static mode." For example, if the configured rate is 1 Mbps, the rate limit of each client online is 1 Mbps. When the set rate limit multiplied by the number of access clients exceeds the available bandwidth provided by the AP, no clients can get the guaranteed bandwidth.

Configuration procedure

You can configure WLAN service-based client rate limiting, so that the fat AP can limit client rates for a WLAN service.

To configure WLAN service-based client rate limiting:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter service template view.	**wlan service-template** *service-template-number* { **clear** | **crypto** }	N/A
3. Configure WLAN service-based client rate limiting.	**client-rate-limit direction** { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*	By default, WLAN service-based client rate limiting is disabled.

Displaying and maintaining client rate limiting

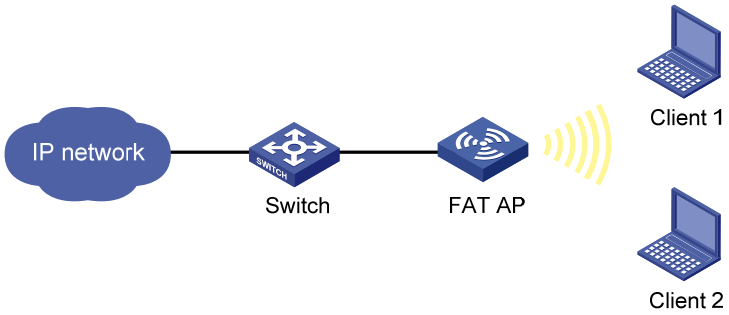
Task	Command	Remarks
Display client rate limiting information.	**display wlan client-rate-limit service-template** [*service-template-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

Client rate limiting configuration example

Network requirements

The fat AP is connected to Switch. Configure client rate limiting on the fat AP, so that fat AP limits the incoming traffic in static mode and limits the outgoing traffic in dynamic mode for the clients.

Figure 32 Network diagram



Configuration procedure

Create a WLAN-ESS interface.

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

Create a WLAN service template of the clear type, configure its SSID as **service**, and enable open-system authentication for the WLAN service template.

```
[AP] wlan service-template 1 clear
[AP-wlan-st-1] ssid service
[AP-wlan-st-1] authentication-method open-system
```

Configure WLAN service-based client rate limiting on AC to limit the rate of traffic from clients to AP (incoming traffic) to 8000 kbps in static mode and the rate of traffic from AP to clients (outgoing traffic) to 8000 kbps in dynamic mode.

```
[AP-wlan-st-1] client-rate-limit direction inbound mode static cir 8000
[AP-wlan-st-1] client-rate-limit direction outbound mode dynamic cir 8000
[AP-wlan-st-1] service-template enable
[AP-wlan-st-1] quit
```

Bind service template 1 to WLAN-BSS 1 on interface WLAN-radio 2/0.

```
[AP] interface wlan-radio 2/0
[AP-WLAN-Radio2/0] radio-type dot11g
[AP-WLAN-Radio2/0] channel 1
[AP-WLAN-Radio2/0] service-template 1 interface wlan-bss 1
[AP-WLAN-Radio2/0] return
```

Verifying the configuration

Use the **display wlan client-rate-limit service-template** command to display the client rate limiting configuration.

```
<AP> display wlan client-rate-limit service-template
                            Client Rate Limit
--------------------------------------------------------------------------------
 Service Template       Direction       Mode            CIR(kbps)
--------------------------------------------------------------------------------
```

```
 1                     Inbound         Static          8000
 1                     Outbound        Dynamic         8000
--------------------------------------------------------------------------------
```

1. When only Client 1 accesses the WLAN through SSID **service**, the available bandwidth is limited to around 8000 kbps.

2. When both Client 1 and Client 2 access the WLAN through SSID **service**, the bandwidth available for the traffic from either Client 1 or Client 2 to the AP is limited to around 8000 kbps, and the bandwidth available for the traffic from the AP to either Client 1 or Client 2 is limited to around 4000 kbps.

Index