

User Guide

AX3000 Wi-Fi 6 In-Wall Access Point

Pro-6-IW

IP-COM
World Wide Wireless

Copyright Statement

©2022 IP-COM Networks Co., Ltd. All rights reserved.

IP-COM is the registered trademark of IP-COM Networks Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to IP-COM Networks Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of IP-COM Networks Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Thank you for choosing IP-COM! This user guide walks you through all functions on the Web UI of AX3000 Wi-Fi 6 In-Wall Access Point. All the screenshots herein, unless otherwise specified, are taken from Pro-6-IW.

Conventions

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	System > Live Users
Button	Bold	Click the OK button.
Parameter and value	Bold	Set User Name to Tom .
Variable	Italic	Format: <i>XX:XX:XX:XX:XX:XX</i>

The symbols that may be found in this document are defined as follows.

Symbol	Meaning
 Note	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to the device.
 Tip	This format is used to highlight a procedure that will save time or resources.

For More Documents

Search target product models on our official website www.ip-com.com.cn to obtain the latest product documents.

Product document overview

Document	Overview
Datasheet	Walks you through basic parameters such as product overview, product features, and specifications of APs.
Quick Installation Guide	Walks you through a rapid AP network establishment, including AP installation, network configuration, LED/Port/Button description, FAQ, and so on.
User Guide	Walks you through detailed functions and configurations of APs, including all the functions on the web UI.

Technical Support

If you need more help, contact us by any of the following means. We will be glad to assist you as soon as possible.



+86-755-27653089



info@ip-com.com.cn



www.ip-com.com.cn

Revision History

IP-COM is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the user guide was released.

Version	Date	Description
V1.0	2022-06-30	Original publication.

Contents

1 Log in to the Web UI	1
1.1 Login	1
1.2 Logout	3
2 Web UI	4
2.1 Layout	4
2.2 Common Buttons	5
3 Quick Setup	6
3.1 AP Working Mode	6
3.1.1 Overview	6
3.1.2 Quick Setup	7
3.2 Client+AP Working Mode	8
3.2.1 Overview	8
3.2.2 Quick Setup	8
4 Status	11
4.1 System Status	11
4.2 Wireless Status	13
4.3 Traffic Statistics	14
4.4 Client List	15
5 Internet Settings	16
6 Wireless	18
6.1 SSID settings	18
6.1.1 Overview	18
6.1.2 Example of Setting up an Open Wireless Network	25
6.1.3 Example of Setting up a Wireless Network Encrypted with PSK	27
6.1.4 Example of Setting up a Wireless Network Encrypted with WPA or WPA2	29

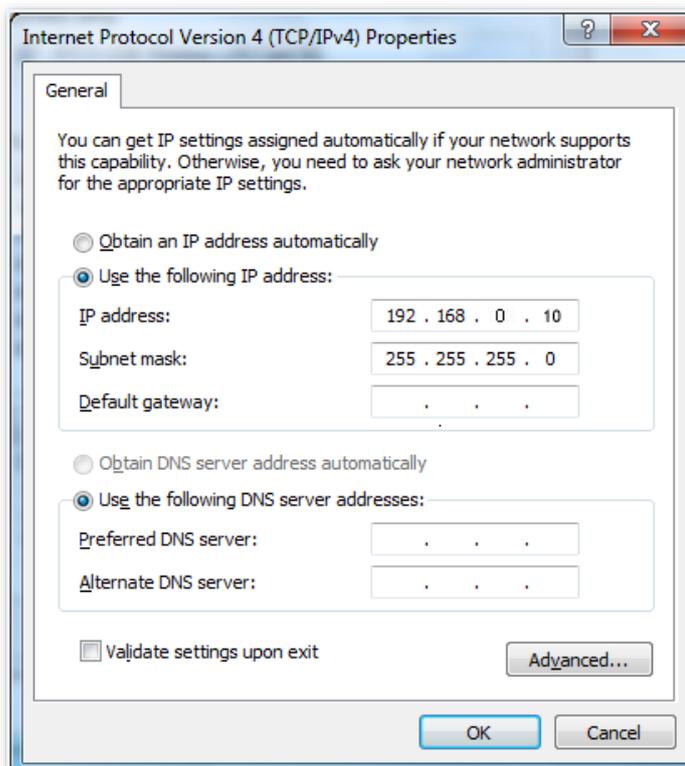
6.2 RF Settings	45
6.3 RF Optimization	48
6.4 Frequency Analysis	52
6.4.1 Overview	52
6.4.2 View Frequency Analysis	52
6.4.3 Execute Channel Scan	53
6.5 WMM.....	54
6.5.1 Overview	54
6.5.2 Configure WMM settings	55
6.6 Access Control	57
6.6.1 Overview	57
6.6.2 Configure Access Control	57
6.6.3 Example of Configuring Access Control	58
6.7 Advanced Settings	60
6.7.1 Overview	60
6.7.2 Configure Advanced Settings	61
6.8 QVLAN Settings.....	62
6.8.1 Overview	62
6.8.2 Configure the QVLAN Function	63
6.8.3 Example of Configuring QVLAN Settings.....	65
7 Advanced	68
Traffic Control	68
Configure Traffic Control	69
8 Tools	70
8.1 Date & Time	70
8.1.1 System Time	70
8.1.2 Login Timeout Interval	71
8.2 Maintenance.....	72
8.2.1 Reboot.....	72
8.2.2 Reset.....	74

8.2.3 Upgrade Firmware	75
8.2.4 Backup/Restore	76
8.2.5 LED Indicator Control	78
8.3 Account.....	80
8.3.1 Overview	80
8.3.2 Modify the password and user name of login account	81
8.4 System Log.....	82
8.5 Diagnostic Tool.....	83
8.6 Uplink Detection	84
8.6.1 Overview	84
8.6.2 Configure Uplink Detection.....	85
Appendixes	86

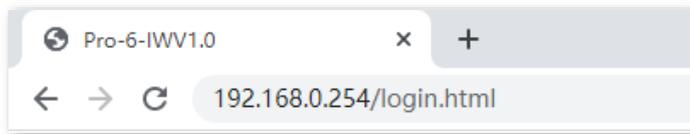
1 Log in to the Web UI

1.1 Login

1. Use an Ethernet cable to connect the computer to the Access Point or the switch connected to the AP.
2. Configure the IP address of the computer to one in a same network segment with the AP. For example, if IP address of the AP is **192.168.0.254**, then the IP address of the computer can be Set to **192.168.0.X** (X ranges from 2 to 253 and is not occupied by other devices) and subnet mask can be set to **255.255.255.0**.



3. Start a browser on the computer and visit the IP address of the AP (**192.168.0.254** by default).



4. Enter the login user name and password, and click **Login**.

 A screenshot of the "Access Point" login page. The page has a title "Access Point" in red. Below the title are three input fields: "Default user name: admin", "Default password: admin" (with a toggle for visibility), and "English" (with a dropdown arrow). Below these fields is a red "Login" button and a link for "Forgot password?".

---End



If the above page does not appear, try the following solutions:

- Ensure that all your Ethernet cables are properly connected.
- Clear the cache of your web browser, or try with the web browser.
- Ensure that the IP address of the computer is in a same network segment with the AP.
- The AP may obtain an IP address from a DHCP server in the LAN. You can check the new IP address from the client list of the DHCP server and use this new IP address to log in.
- If two or more APs are connected in a network without a controller, connect one AP to the network first, change its IP address to a different IP address on the same network segment, and then connect to the next AP and proceed the same modifications.
- If the problem persists, reset the AP, and then try logging in again. How to reset: After AP completes startup, hold down the reset button for about 10 seconds, and release when the indicator goes out. When the indicator blinks white, the AP is reset.

Log in to the web UI of the AP. You can configure the AP now.

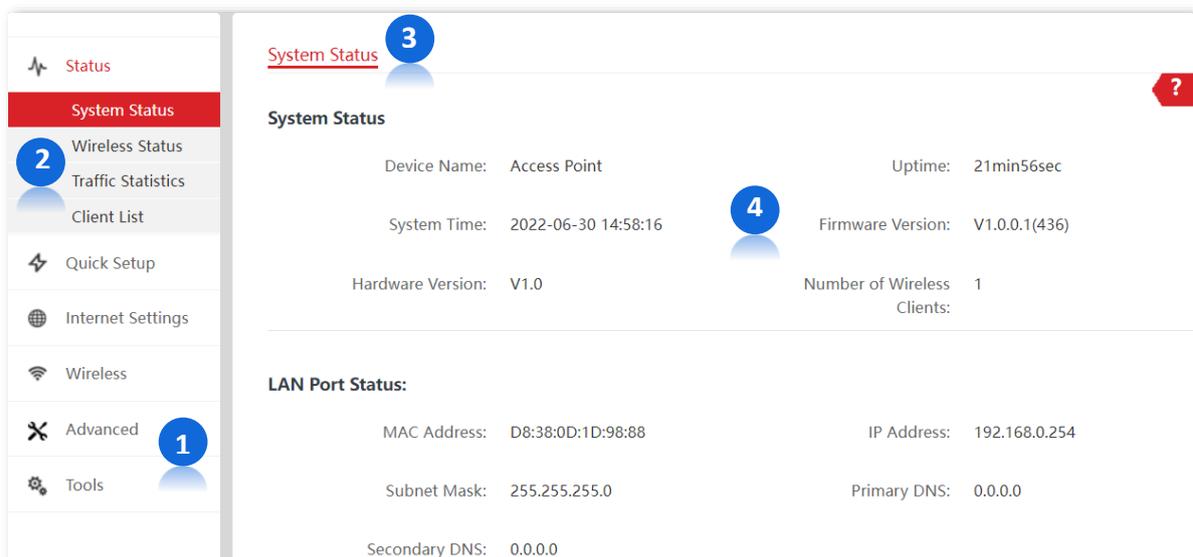
1.2 Logout

After you log in to the web UI of the AP, if no operations are performed during the [login timeout interval](#), the system will log out automatically. In addition, you can click **Logout** on the upper right corner to safely exit from the web UI.

2 Web UI

2.1 Layout

The web UI is composed of four parts: first-level navigation bar, second-level navigation bar, tab, and configuration area, as shown below.



Tip

Functions or parameters displayed in gray on the web UI are not supported yet or cannot be modified under the current configurations.

No.	Name	Description
1	First-level navigation bar	Function menu that organizes AP by navigation tree and tab. You can choose the function menu as needed and the result appears on the configuration area.
2	Second-level navigation bar	
3	Tab	
4	Configuration area	Area where you perform or check configurations.

2.2 Common Buttons

Buttons commonly used on the web UI are illustrated as below.

Common button	Description
	Refresh the current page.
	Save configurations on the current page and make the configurations take effect.
	Cancel the unsaved configurations on the current page and restore to previous configurations.
	Check the help information of the current page.

3 Quick Setup

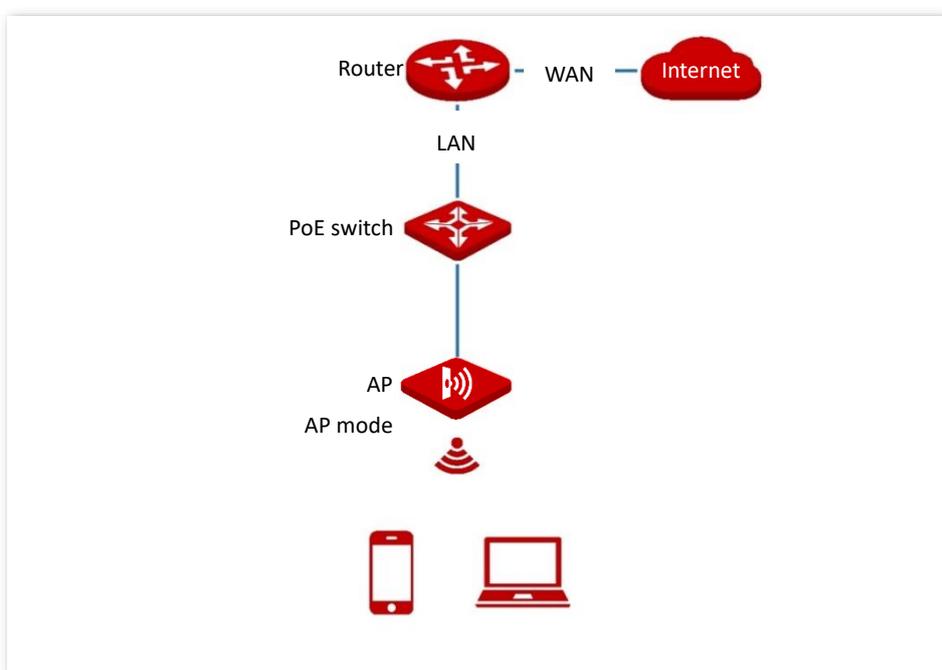
In the **Quick Setup** module, you can set up the AP in a quick way to enable internet access for your wireless devices such as smartphones and tablets.

The AP supports working modes of [AP](#) and [Client+AP](#).

3.1 AP Working Mode

3.1.1 Overview

In this mode, AP connects to the internet using an Ethernet cable and transforms wired signals to wireless signals for wireless coverage. AP works under this mode by default. See the following topology.



3.1.2 Quick Setup



Before configuration, ensure that the upstream router has been connected to the internet.

1. Click **Quick Setup**.
2. Choose the **Radio Band** you wish to configure, for example, **2.4GHz**.
3. Set **Working Mode** to **AP**.
4. Set **SSID** ([Primary SSID](#)).
5. Select **Security Mode** and configure the incurred parameters.
6. Click **Save**.

7. If you need to configure the other radio band, repeat **steps 2** to **6**.

---End

Search and connect your wireless devices such as smartphones to the **SSID** you set. Enter the wireless password (the **Key** you set) and you will be able to access the internet.

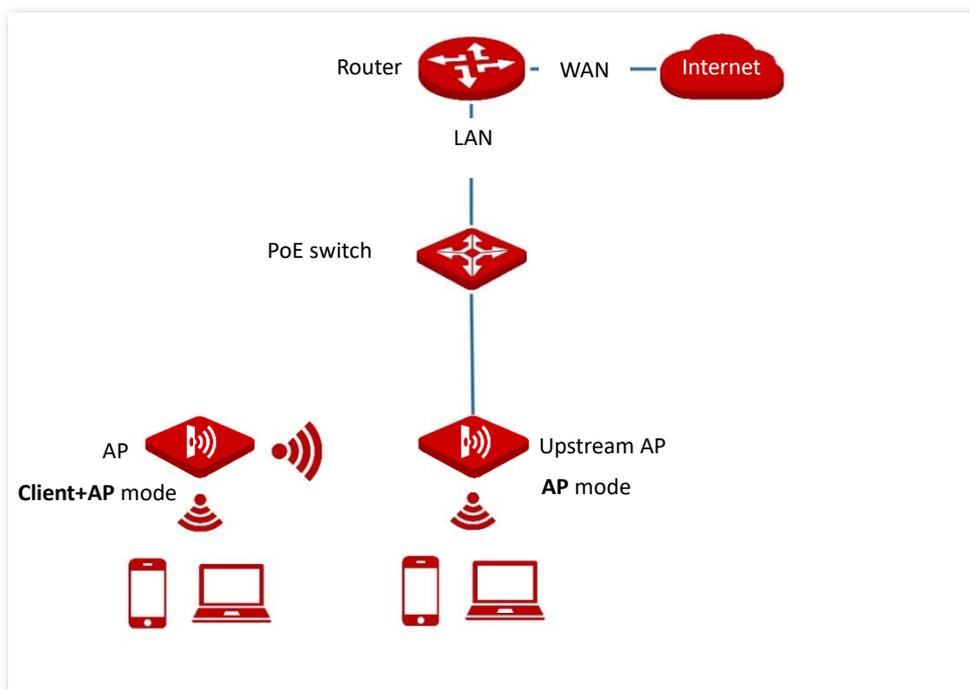
Parameter description

Parameter	Description
Radio Band	Select the radio band you wish to configure.
Working Mode	Choose the AP mode to convert wired networks into wireless networks.
SSID	Click to modify the WiFi name of the primary network under the selected radio band.
Security Mode	Select the security modes for target wireless networks. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode: None , WEP , WPA-PSK , WPA2-PSK , Mixed WPA/WPA2-PSK , WPA , WPA2 , WPA3-SAE , WPA2-PSK&WPA3-SAE .

3.2 Client+AP Working Mode

3.2.1 Overview

In this mode, the AP is wirelessly bridged to an upstream device (such as a wireless router or AP) to extend the wireless network coverage of the upstream device. See the following topology.



3.2.2 Quick Setup



Tip

Before configuration, ensure that the upstream AP has been connected to the internet.

1. Choose **Quick Setup**.
2. Select the radio band from the drop-down list box, which is **2.4 GHz** in this example.
3. Set **Working Mode** to **Client+AP**.
4. Click **Scan**.

Quick Setup

Radio Band

Working Mode AP Client+AP

SSID

Security Mode

- Select the wireless network to be extended from the wireless network list that appears.



- If no wireless network is found, choose **Wireless > RF Settings**, ensure that **Wireless Network** is selected, and try scanning wireless network again.
- After a wireless network to be extended is selected, the SSID, security mode, and channel of the wireless network are populated automatically.

Select	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
<input type="radio"/>	NOVA_MUY2_A3	C8:3A:35:9A:3B:5A	20	10	WPA2-PSK/AES	
<input type="radio"/>	IP-COM_AP_jy	D8:38:0D:D0:01:F3	40	9	WPA-PSK/AES	
<input checked="" type="radio"/>	EW15D	D8:38:0D:EE:43:99	20	12	WPA2-PSK/AES	

- Click **Disable**.
- If the wireless network of the upstream device is encrypted, enter the wireless network password of the device in the **Key** column.
- Click **Save**.

Quick Setup ?

Radio Band

Working Mode AP Client+AP

SSID

Security Mode

Encryption Algorithm AES TKIP TKIP&AES

Key

---End

After the configuration, you can select the SSID on your wireless devices such as smartphones and enter your wireless network password to connect to the wireless network of the AP and access the internet through the AP.



Tip

If you do not know the SSID and key of the AP, you can check the SSID and key of the AP on the **Wireless > SSID** page.

Parameter description

Parameter	Description
Radio Band	It specifies the radio band for configurations.
Working Mode	Choose the Client+AP mode to bridge the upstream WiFi network.
SSID	It specifies the WiFi network name (SSID) of the WiFi network to be bridged. After you select the upstream WiFi network from the scanned wireless network list, this parameter will be populated automatically.

It specifies the security mode of which the upstream WiFi network adopted. See [Security Mode](#) for details.



Note

Security Mode

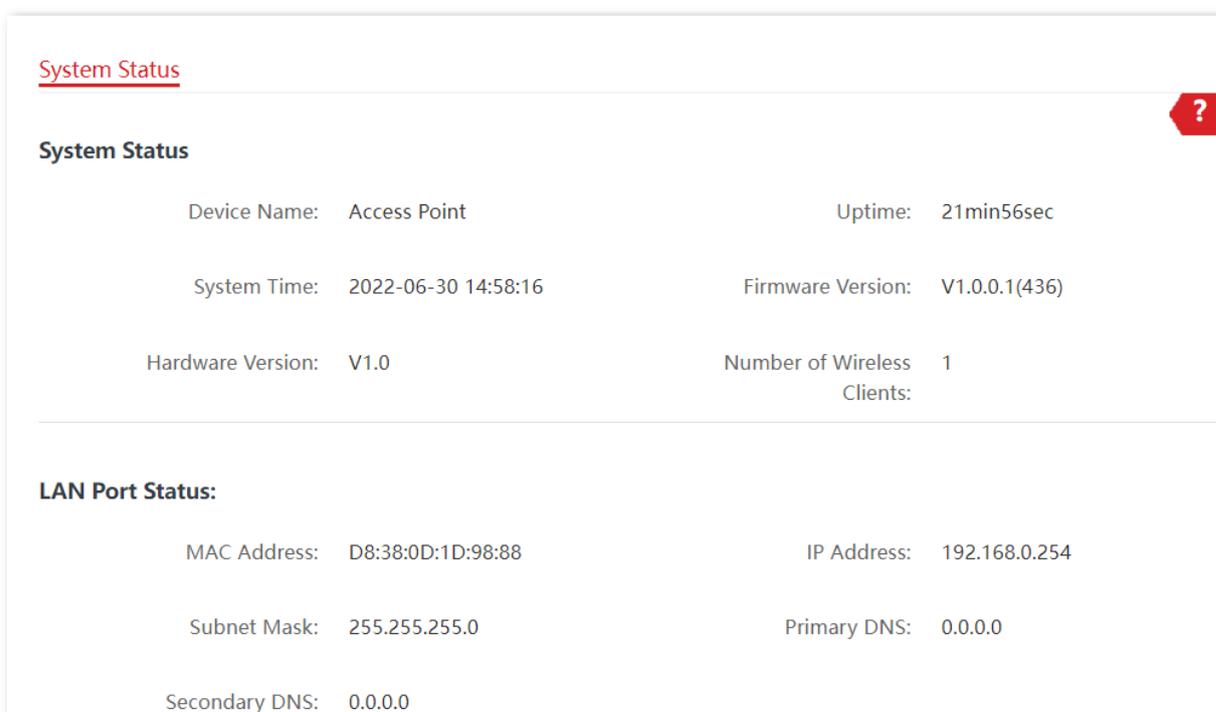
- If the wireless network to be bridged adopts the **WEP** security mode, **Authentication Type**, **Default Key**, and **Key x** (x ranges from 1 to 4) need to be entered manually.
- If the wireless network to be bridged adopts the WPA-PSK, WPA2-PSK or Mixed WPA/WPA2-PSK security mode, **Encryption Algorithm** will be populated automatically and you only need to enter the **Key**.

4 Status

4.1 System Status

To access the page, choose **Status** > **System Status**.

The page displays the system and LAN port status of the AP.



The screenshot shows a web interface for 'System Status'. At the top left, the title 'System Status' is underlined in red. In the top right corner, there is a red arrow pointing left with a white question mark. The main content is divided into two sections: 'System Status' and 'LAN Port Status:'. The 'System Status' section contains six items arranged in two columns: Device Name: Access Point, Uptime: 21min56sec, System Time: 2022-06-30 14:58:16, Firmware Version: V1.0.0.1(436), Hardware Version: V1.0, and Number of Wireless Clients: 1. The 'LAN Port Status:' section contains four items: MAC Address: D8:38:0D:1D:98:88, IP Address: 192.168.0.254, Subnet Mask: 255.255.255.0, and Primary DNS: 0.0.0.0. A Secondary DNS field is also present with the value 0.0.0.0.

<u>System Status</u>			
System Status			
Device Name:	Access Point	Uptime:	21min56sec
System Time:	2022-06-30 14:58:16	Firmware Version:	V1.0.0.1(436)
Hardware Version:	V1.0	Number of Wireless Clients:	1
LAN Port Status:			
MAC Address:	D8:38:0D:1D:98:88	IP Address:	192.168.0.254
Subnet Mask:	255.255.255.0	Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0		

Parameter description

Parameter	Description	
System Status	Device Name	It specifies the name of the AP. A unique AP name helps quickly identify the AP. You can change the AP name on the LAN Setup page.
	Uptime	It specifies the time that has elapsed since the AP was started last time.
	System Time	It specifies the current system time of the AP.
	Firmware Version	It specifies the firmware version of the AP.
	Hardware Version	It specifies the hardware version of the AP.
	Number of Wireless Clients	It specifies the number of wireless clients currently connected to the AP.
LAN Port Status	MAC Address	It specifies the physical address of the LAN port of the AP. If you connect the AP to other devices using Ethernet cables, the AP uses this MAC address to communicate with those devices.
	IP Address	It specifies the IP address of the AP and it is also the management IP address of the AP. The web UI of the AP is accessible by visiting this IP address. You can change the IP address on the LAN Setup page.
	Subnet Mask	It specifies the subnet mask of the IP address of the AP.
	Primary DNS	It specifies the primary DNS server of the AP.
	Secondary DNS	It specifies the secondary DNS server of the AP.

4.2 Wireless Status

To access the page, choose **Status > Wireless Status**.

This page displays general radio status and SSID status of the AP. By default, the page displays the information of 2.4 GHz wireless status. To view the wireless status of 5 GHz, click **5 GHz**.

[2.4 GHz](#) [5 GHz](#)
?

RF Status

RF: Enabled Network Mode: 11b/g/n/ax

Channel: 12

SSID Status

SSID	MAC Address	Status	Security Mode
IP-COM_18B02A	D8:38:0D:18:B0:2A	Enabled	None
IP-COM_18B02B	D8:38:0D:18:B0:2B	Disabled	None
IP-COM_18B02C	D8:38:0D:18:B0:2C	Disabled	None
IP-COM_18B02D	D8:38:0D:18:B0:2D	Disabled	None
IP-COM_18B02E	D8:38:0D:18:B0:2E	Disabled	None
IP-COM_18B02F	D8:38:0D:18:B0:2F	Disabled	None
IP-COM_18B020	D8:38:0D:18:B0:20	Disabled	None
IP-COM_18B021	D8:38:0D:18:B0:21	Disabled	None

Parameter description

Parameter	Description	
RF Status	RF	It specifies whether the wireless function of the AP is enabled.
	Network Mode	It specifies the current network mode of the AP.
	Channel	It specifies the current working channel of the AP.
SSID Status	SSID	It specifies the names of all the wireless networks of the AP.
	MAC Address	It specifies the physical addresses corresponding to the SSIDs of the AP.
	Status	It specifies whether the wireless networks corresponding to the SSIDs of the AP are enabled.
	Security Mode	It specifies the security modes of the wireless networks corresponding to the SSIDs of the AP.

4.3 Traffic Statistics

To access the page, choose **Status > Traffic Statistics**.

This page displays the statistics about historical packets of the wireless networks of the AP.

By default, the page displays the traffic statistics information of 2.4 GHz. To view information about 5 GHz, click **5 GHz**.

<u>2.4 GHz</u> <u>5 GHz</u>				
SSID	Received Traffic	Received Packets (Qty.)	Transmitted Traffic	Transmitted Packets (Qty.)
IP-COM_18B02A	0.01MB	74	0.93MB	10433
IP-COM_18B02B	0.00MB	0	0.00MB	0
IP-COM_18B02C	0.00MB	0	0.00MB	0
IP-COM_18B02D	0.00MB	0	0.00MB	0
IP-COM_18B02E	0.00MB	0	0.00MB	0
IP-COM_18B02F	0.00MB	0	0.00MB	0
IP-COM_18B020	0.00MB	0	0.00MB	0
IP-COM_18B021	0.00MB	0	0.00MB	0

Parameter description

Parameter	Description
SSID	It specifies the wireless network name.
Received Traffic	It specifies the total number of bytes received by a wireless network.
Received Packets (Qty.)	It specifies the total number of packets received by a wireless network.
Transmitted Traffic	It specifies the total number of bytes transmitted by a wireless network.
Transmitted Packets (Qty.)	It specifies the total number of packets transmitted by a wireless network.



All the statistics are cleared when the wireless function is disabled or this device is rebooted. All the wireless network statistics of an SSID are cleared when the SSID is disabled.

4.4 Client List

To access the page, choose **Status > Client List**.

This page displays information about the wireless clients connected to the wireless networks of the AP. You can also block certain connected clients.

2.4 GHz 5 GHz

Clients connected to the SSID: SSID:

ID	MAC Address	IP Address	Client Type	Connection Duration	Transmit Rate	Receive Rate	Block
1	7E:99:B6:51:C7:03	192.168.0.60	IOS	00:00:03	907Mbps	6Mbps	

in total/Page 1 in total

Parameter description

Parameter	Description
SSID	Select the SSID from the drop-down list menu to view client information connected to it.
MAC Address	It specifies the MAC address of the wireless client.
IP Address	It specifies the IP address of the wireless client.
Client Type	It specifies the operating system of the wireless client. <div style="display: flex; align-items: center;">  Tip </div> The operating system type of the client can be identified only when AP is enabled with the Identify Client Type function and the client has visited a HTTP website.
Connection Duration	It specifies the online duration of the wireless client.
Transmit Rate	It specifies the current transmit speed of the wireless client.
Receive Rate	It specifies the current receive speed of the wireless client.
Block	Click  to block the client from accessing the AP's wireless network. To view the disconnected client, choose Wireless > Access Control .

5 Internet Settings

To access the page, choose **Internet Settings > LAN Setup**.

This page enables you to view the MAC address of the LAN port of the AP and set the name, Ethernet Mode, IP obtaining method, and other related parameters of the AP.

LAN Setup ?

MAC Address D8:38:0D:1D:98:88

IP Address Type Static IP

IP Address 192.168.0.254

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

Primary DNS 0.0.0.0

Secondary DNS 0.0.0.0

Device Name Access Point

Optimize Ethernet for: Faster Speed (Auto Negotiation)
 Longer Distance (10 Mbps Full Duplex)

Save Cancel

Parameter description

Parameter	Description
MAC Address	It specifies the MAC address of the LAN port of the AP.
IP Address Type	<p>It specifies the IP address obtaining mode of the AP.</p> <ul style="list-style-type: none"> – Static IP: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP are set manually. It is proper for the scenarios where only one or several APs are required in the network. – DHCP (Dynamic IP Address): It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is obtained from a DHCP server on your LAN. It is proper for the scenarios where a large group of

Parameter	Description
	APs are required in the network.
	 Tip If Address Type is set to DHCP (Dynamic IP Address) , you can log in to the web UI of the AP only with the IP address assigned to the AP by the DHCP server. The IP address is specified on the client list of the DHCP server.
IP Address	It specifies the IP address of the AP. The web UI of the AP is accessible at this IP address.
Subnet Mask	It specifies the subnet mask of the IP address of the AP.
Default Gateway	It specifies the gateway IP address of the AP. Generally, set the gateway IP address to the LAN IP address of your LAN router connected to the internet, so that the AP can access the internet.
Primary DNS	It specifies the primary DNS server of the AP. If your LAN router connected to the internet provides the DNS proxy function, this IP address can be the LAN IP address of the router. Otherwise, enter a correct DNS server IP address.
Secondary DNS	It specifies the IP address of the secondary DNS server of the AP. This parameter is optional. If a DNS server IP address in addition to the IP address of the primary DNS server is available, enter the additional IP address in this field.
Device Name	It specifies the name of the AP. You are recommended to change the name of the AP to indicate the location of the AP (such as Bedroom), so that you can easily identify the AP when managing many APs.
	It specifies the Ethernet mode of the PoE LAN port of this AP. <ul style="list-style-type: none"> – Faster Speed (Auto Negotiation): This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended. – Longer Distance (10 Mbps Full Duplex): This mode features a long transmission distance but relatively low transmission rate (usually 10 Mbps).
Optimize Ethernet for	 Tip <ul style="list-style-type: none"> – The 10 Mbps Full Duplex mode is recommended only when the Ethernet cable that connects the PoE LAN port of the AP to a peer device exceeds 100 meters. In this case, the connected LAN port of the peer device must work in auto-negotiation mode. Otherwise, the PoE LAN port of the AP may not be able to properly transmit or receive data. – Modifications to Ethernet mode take effect after you reboot the AP or unplug from and plug into the port again.

6 Wireless

6.1 SSID settings

6.1.1 Overview

To access the page, choose **Internet Settings** > **LAN Setup**.

This module enables you to set SSID-related parameters of the AP.

2.4 GHz 5 GHz

SSID

Status Enable Disable

Broadcast SSID Enable Disable

Isolate Client Enable Disable

Isolate SSID Enable Disable

WMF Enable Disable

Max. Number of Clients (Range: 1 to 128)

SSID

Chinese SSID Encoding

Security Mode

Parameter description

Parameter	Description
SSID	It specifies the SSID to be configured. APs of this series support 8 SSIDs for the 2.4 GHz radio band and 8 SSIDs for the 5 GHz radio band. The first SSID displayed on the page under the radio band tab is the primary SSID of the radio band.

Parameter	Description
Status	It specifies the status of the selected SSID. Primary SSID is enabled by default while other SSIDs are disabled by default. You can enable them as needed.
Broadcast SSID	It specifies the broadcast status of the SSID you selected. When this parameter is set to Disable , the AP does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. This enhances the security of the wireless network.
Isolate Client	It specifies whether to isolate clients connected to the same SSID. When this parameter is set to Enable , it isolates the wireless clients connected to the same wireless network corresponding to an SSID, so that the wireless clients can access only the wired network connected to the AP. Applying this function to hotspot setup at public places such as hotels and airports helps increase network security.
Isolate SSID	It specifies whether to isolate the wireless clients connected to the AP with different SSIDs. When this parameter is set to Enable , devices connected to different SSIDs cannot communicate with each other.
WMF	It specifies whether to enable the WMF function. The WMF function of the AP converts multicast traffic into unicast traffic and forwards the traffic to the multicast traffic destination in the wireless network. This helps save wireless resources, ensure reliable transmission, and reduce delays.
Max. Number of Clients	It specifies the maximum number of clients that can be concurrently connected to the wireless network corresponding to an SSID. If the number is reached, new devices cannot connect to the SSID unless some devices cut off their connections.
SSID	Click it to modify the selected SSID (name of the wireless network).
Chinese SSID Encoding	It specifies the encoding format of Chinese characters in an SSID. The default value is UTF-8 . If multiple SSIDs of the AP are enabled and contain Chinese characters, you are recommended to set this parameter to UTF-8 for some SSIDs and to GB2312 for others, so that any wireless clients can identify these SSIDs.
Security Mode	It specifies the security mode of the selected SSID. The options include: None , WEP , WPA-PSK , WPA2-PSK , Mixed WPA/WPA2-PSK , WPA , WPA2 , WPA3-SAE , WPA2-PSK&WPA3-SAE .

Security Mode

A wireless network uses radio, which is open to the public, as its data transmission medium. If the wireless network is not protected by necessary measures, any client can connect to the network to use the resources of the network or access unprotected data over the network. To ensure communication security, transmission links of wireless networks must be encrypted for protection.

The AP supports various security modes for network encryption, including [None](#), [WEP](#), [WPA-PSK](#), [WPA2-PSK](#), [Mixed WPA/WPA2-PSK](#), [WPA](#), [WPA2](#), [WPA3-SAE](#), [WPA2-PSK&WPA3-SAE](#).

- **None**

It indicates that any wireless client can connect to the wireless network. This option is not recommended because it affects network security.

- **WEP**

It uses a static key to encrypt all exchanged data, and ensures that a wireless LAN has the same level of security as a wired LAN. Data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum wireless network throughput of only 54 Mbps. Therefore, this security mode is not recommended.

Security Mode	WEP ▾	
Authentication Type	Open ▾	
Default Key	Key 1 ▾	
Key 1	ASCII ▾
Key 2	ASCII ▾
Key 3	ASCII ▾
Key 4	ASCII ▾

Parameter description

Parameter	Description
Authentication Type	<p>It specifies the authentication type for the WEP security mode. The options include Open, Shared. The options share the same encryption process.</p> <ul style="list-style-type: none"> – Open: It specifies that authentication is not required and data exchanged is encrypted with WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. – Shared: It specifies that a shared key is used for authentication and data exchanged is encrypted with WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key.
Default Key	<p>It specifies the WEP key for the Open or Shared encryption type.</p> <p>For example, if Default Key is set to Key 2, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Key 2.</p>
Key 1/2/3/4	<p>4 WEP keys are allowed at the same time, but only the one specified by the Default Key is valid. The key type includes ASCII and Hexadecimal.</p> <ul style="list-style-type: none"> – ASCII: 5 or 13 ASCII characters are allowed in the key. – Hex: 10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key.

■ WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK

They belong to pre-shared key or personal key modes, where Mixed WPA/WPA2-PSK supports both WPA-PSK and WPA2-PSK.

WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK adopt a pre-shared key for authentication, while the AP generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home wireless networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all clients use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.

The screenshot shows a configuration window for wireless security. The 'Security Mode' dropdown is set to 'WPA-PSK'. A list of options is displayed, including 'None', 'WEP', 'WPA-PSK', 'WPA2-PSK', 'Mixed WPA/WPA2-PSK', 'WPA', 'WPA2', 'WPA3-SAE', and 'WPA2-PSK&WPA3-SAE'. The 'WPA-PSK' option is highlighted with a blue selection bar. To the right, 'Encryption Algorithm' is set to 'TKIP&AES'. Below, the 'Key' field is empty, and 'Key Update Interval' is set to 'Second (Range: 60 to 99999. 0 indicates no upgrade)'.

Parameter description

Parameter	Description
Security Mode	<p>It specifies the personal or pre-shared key security mode.</p> <ul style="list-style-type: none"> – WPA-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA-PSK. – WPA2-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA2-PSK. – Mixed WPA/WPA2-PSK: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK.
Encryption Algorithm	<p>It specifies the encryption algorithm corresponding to the selected security mode. If Security Mode is set to WPA-PSK, this parameter can be set to AES and TKIP values. If Security Mode is set to WPA2-PSK or Mixed WPA/WPA2-PSK, this parameter can be set to AES, TKIP, and TKIP&AES values.</p> <ul style="list-style-type: none"> – AES: It indicates the Advanced Encryption Standard. – TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. – TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a pre-shared WPA key, that is, the password clients use to connect to the wireless network.
Key Update Interval	<p>It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.</p> <p>The value 0 indicates that a WPA key is not updated.</p>

■ WPA, WPA2

To address the key management weakness of WPA-PSK and WPA2-PSK, the WiFi Alliance puts forward WPA and WPA2, which use 802.1x to authenticate clients and generate data encryption-oriented root keys. WPA and WPA2 use the root keys to replace the pre-shared keys set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK.

WPA and WPA2 uses 802.1x to authenticate clients and the login information of a client is managed by the client. This effectively reduces the probability of information leakage. In addition, each time a client connects to an AP that adopts the WPA or WPA2 security mode, the RADIUS server generates a data encryption key and assigns it to the client. This makes it difficult for attackers to obtain the key. These features of WPA and WPA2 help significantly increase network security, making WPA and WPA2 the preferred security modes of wireless networks that require high security.

Security Mode	WPA	
RADIUS Server	None WEP WPA-PSK WPA2-PSK Mixed WPA/WPA2-PSK	
RADIUS Port	WPA WPA2 WPA3-SAE WPA2-PSK&WPA3-SAE	(Range: 1025 to 65535. Default: 1812)
RADIUS Key		
Encryption Algorithm	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP&AES	
Key Update Interval	0	Second (Range: 60 to 99999. 0 indicates no upgrade)

Parameter description

Parameter	Description
Security Mode	<p>The WPA and WPA2 options are available for network protection with a RADIUS server.</p> <ul style="list-style-type: none"> – WPA: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA. – WPA2: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA2.
RADIUS Server	
RADIUS Port	It specifies the IP address/port number/shared password of the RADIUS server.
RADIUS Key	
Encryption Algorithm	<p>It specifies the encryption algorithm corresponding to the selected security mode. The available options include AES, TKIP, and TKIP&AES.</p> <ul style="list-style-type: none"> – AES: It indicates the Advanced Encryption Standard. – TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. – TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key Update Interval	<p>It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.</p> <p>The value 0 indicates that a WPA key is not updated.</p>

■ WPA3-SAE

It is an upgraded version of WPA2-PSK. With Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF), this security mode provides protection against dictionary attacks and information disclosure, saving you the trouble to set a complicated password.



Tip

If your WiFi enabled devices do not support the WPA3-SAE or you have a poor WiFi experience, you are recommended to switch the security mode back to **WPA2-PSK**.

Security Mode	WPA3-SAE	
Encryption Algorithm	None WEP WPA-PSK WPA2-PSK	TKIP&AES
Key	Mixed WPA/WPA2-PSK WPA WPA2	
Key Update Interval	WPA3-SAE WPA2-PSK&WPA3-SAE	Second (Range: 60 to 99999. 0 indicates no upgrade)

■ WPA2-PSK&WPA3-SAE

It indicates that the AP is compatible with both WPA3-SAE and WPA2-PSK security modes. WPA2 is still widely used currently. To allow wireless devices that do not support WPA3 to access the WPA3 network, the AP supports the WPA3-SAE transition mode, which means that the mixed encryption mode of WPA2-PSK and WPA3-SAE is adopted to ensure both compatibility and security.

Security Mode	WPA2-PSK&WPA3-SAE	
Encryption Algorithm	None WEP WPA-PSK WPA2-PSK	TKIP&AES
Key	Mixed WPA/WPA2-PSK WPA WPA2	
Key Update Interval	WPA3-SAE WPA2-PSK&WPA3-SAE	Second (Range: 60 to 99999. 0 indicates no upgrade)

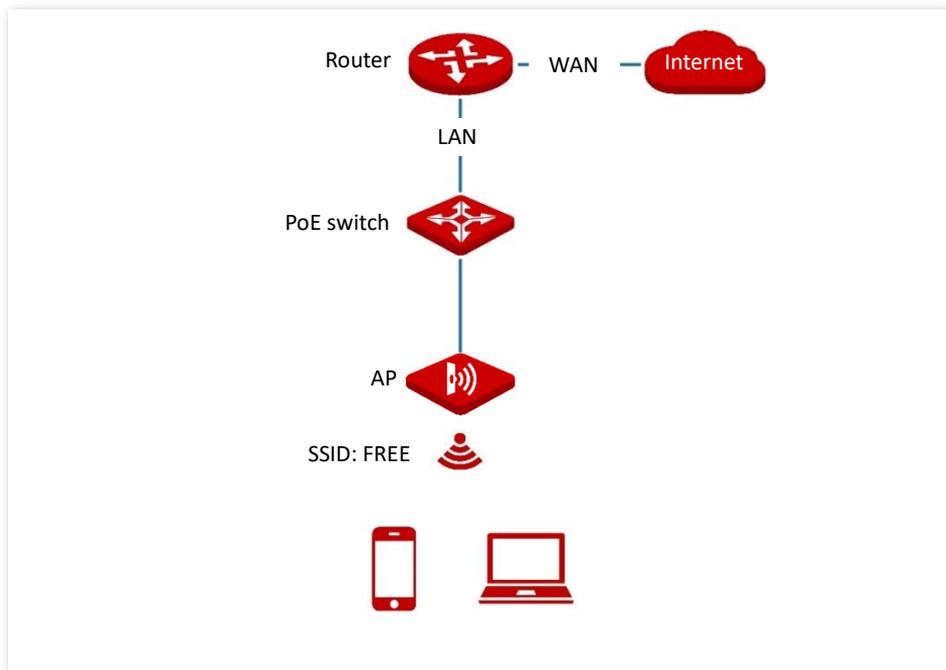
Parameter description

Parameter	Description
Security Mode	<p>Select security mode.</p> <ul style="list-style-type: none"> – WPA3-SAE: The wireless network adopts the WPA3-SAE security mode, which is an upgraded version of WPA2-PSK. – WPA3-SAE/WPA2-PSK: Compatible with WPA3-SAE and WPA2-PSK. At this time, wireless devices can connect to the corresponding wireless network using both WPA3-SAE and WPA2-PSK.
Encryption Algorithm	<p>It specifies the encryption algorithm corresponding to the selected security mode.</p> <ul style="list-style-type: none"> – AES: It indicates the Advanced Encryption Standard. – TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. – TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	<p>It specifies a pre-shared WPA key, that is, the password clients use to connect to the wireless network.</p>
Key Update Interval	<p>It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security.</p> <p>The value 0 indicates that a WPA key is not updated.</p>

6.1.2 Example of Setting up an Open Wireless Network

Networking requirement

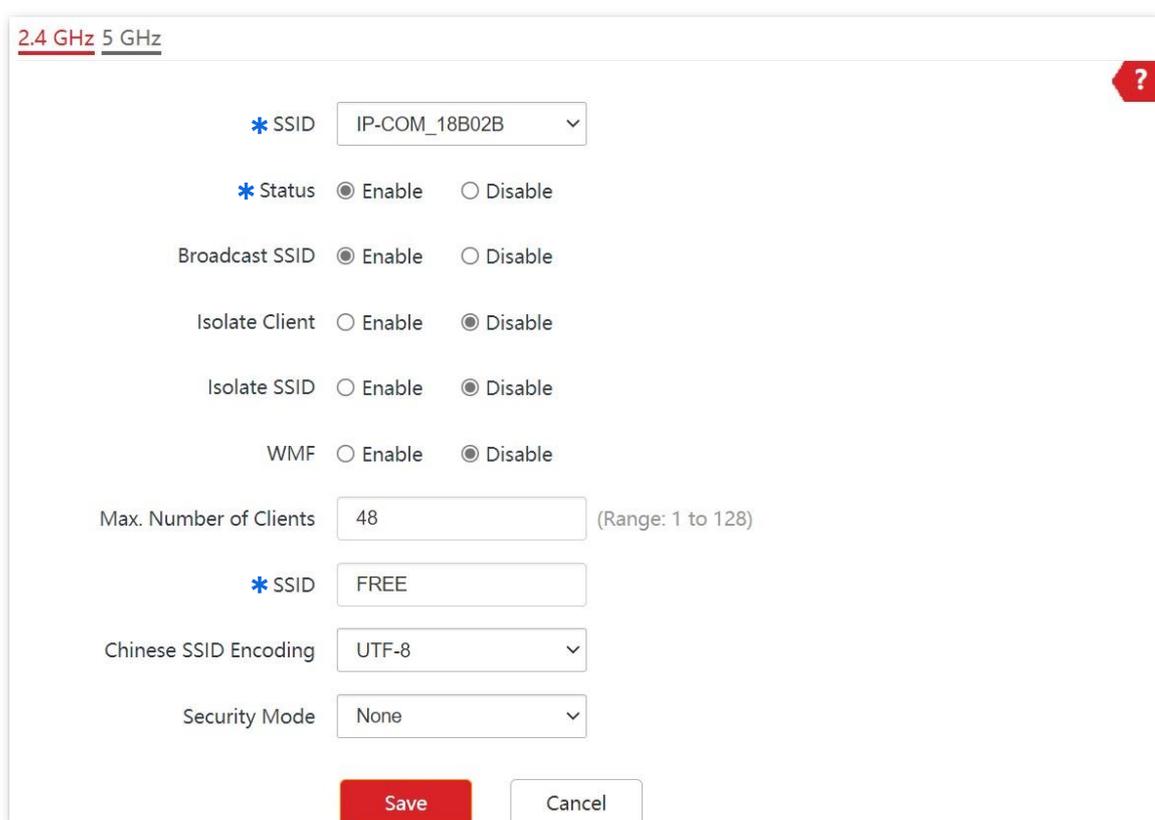
In a hotel lounge, guests can connect to the wireless network without a password and access the internet through the WiFi network.



Configuration procedure

Assume that the second SSID of the 2.4 GHz radio band of the AP is to be configured.

1. Choose **Wireless > SSID**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Set **Status** to **Enable**.
4. Change the value of **SSID** to **FREE**.
5. Set **Security Mode** to **None**.
6. Click **Save**.



The screenshot shows the configuration page for the 2.4 GHz radio band. The page has a header with "2.4 GHz" and "5 GHz" tabs, and a red question mark icon in the top right corner. The configuration options are as follows:

- * SSID: IP-COM_18B02B (dropdown menu)
- * Status: Enable Disable
- Broadcast SSID: Enable Disable
- Isolate Client: Enable Disable
- Isolate SSID: Enable Disable
- WMF: Enable Disable
- Max. Number of Clients: 48 (Range: 1 to 128)
- * SSID: FREE (text input)
- Chinese SSID Encoding: UTF-8 (dropdown menu)
- Security Mode: None (dropdown menu)

At the bottom, there are two buttons: "Save" (red) and "Cancel" (white).

---End

Verification

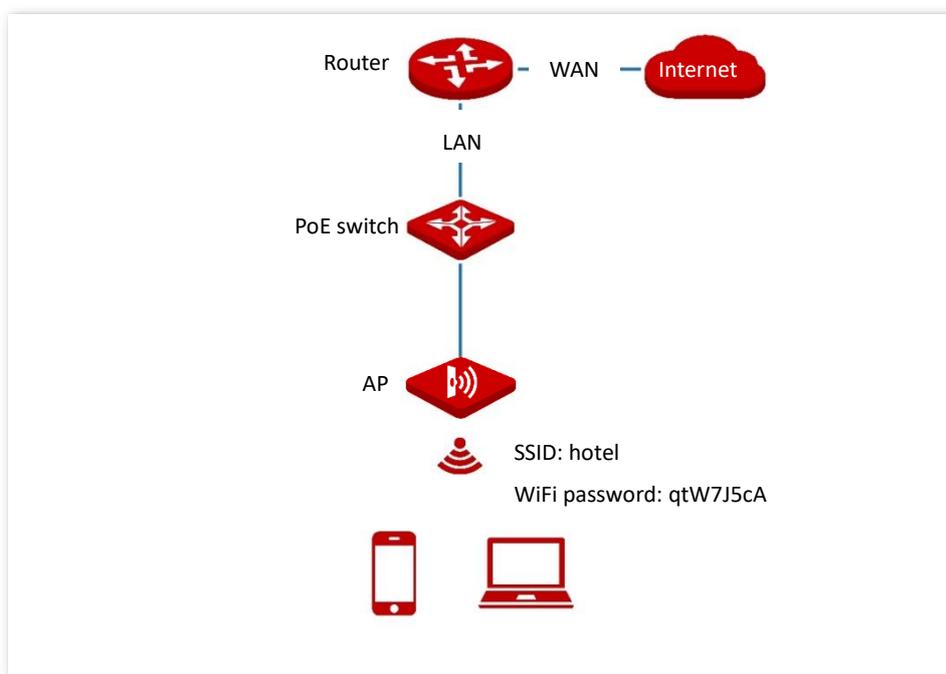
Wireless devices can connect to the **FREE** wireless network without a password.

6.1.3 Example of Setting up a Wireless Network Encrypted with PSK

Networking requirement

A hotel wireless network with a certain level of security must be set up through a simple procedure.

In this case, WPA-PSK, WPA2-PSK or Mixed WPA/WPA2-PSK security mode is recommended. See the following figure.



Configuration procedure

Assume that the second SSID of the AP, the WPA2-PSK security mode, and AES encryption algorithm are used.

1. Choose **Wireless > SSID**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Set **Status** to **Enable**.
4. Change the value of **SSID** to **hotel**.
5. Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.
6. Set **Key** to **qtW7J5cA**.

7. Click Save.

2.4 GHz 5 GHz ?

* SSID

* Status Enable Disable

Broadcast SSID Enable Disable

Isolate Client Enable Disable

Isolate SSID Enable Disable

WMF Enable Disable

Max. Number of Clients (Range: 1 to 128)

* SSID

Chinese SSID Encoding

* Security Mode

* Encryption Algorithm AES TKIP TKIP&AES

* Key

Key Update Interval Second (Range: 60 to 99999. 0 indicates no upgrade)

---End**Verification**

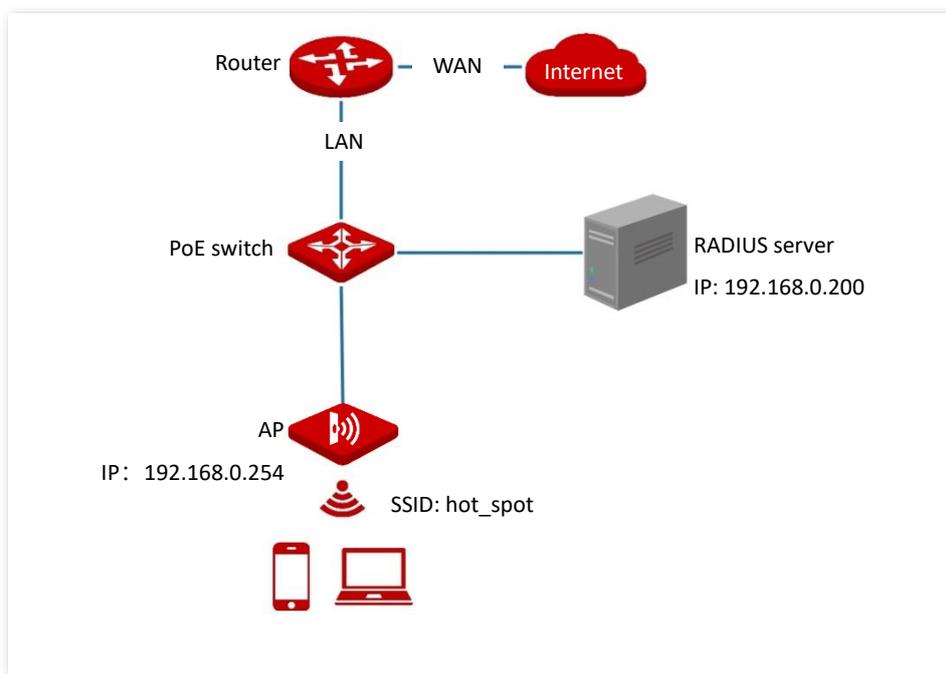
Wireless devices can connect to the **hotel** wireless network with the password **qtW7J5cA**.

6.1.4 Example of Setting up a Wireless Network Encrypted with WPA or WPA2

Networking requirement

A highly secure wireless network is required and a RADIUS server is available. In this case, WPA or WPA2 mode is recommended.

Assume that the IP address of the RADIUS server is **192.168.0.200**, the Key is **qtW7J5cA**, and the port number for authentication is **1812**. See the following figure.



Configuration procedure

I. Configure the AP

Assume that the second SSID of the AP, the WPA2 security mode, and AES encryption algorithm are used.

1. Choose **Wireless > SSID**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Set **Status** to **Enable**.
4. Change the value of **SSID** to **hot_spot**.
5. Set **Security Mode** to **WPA2**.
6. Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Password** to **192.168.0.200**, **1812**, and **qtW7J5cA** respectively.
7. Set **Encryption Algorithm** to **AES**.
8. Click **Save**.

The screenshot shows a configuration page for wireless settings. At the top, there are tabs for '2.4 GHz' and '5 GHz'. A red question mark icon is in the top right corner. The settings are as follows:

- * SSID:** IP-COM_18B02B (dropdown menu)
- * Status:** Enable Disable
- Broadcast SSID:** Enable Disable
- Isolate Client:** Enable Disable
- Isolate SSID:** Enable Disable
- WMF:** Enable Disable
- Max. Number of Clients:** 48 (text input, Range: 1 to 128)
- * SSID:** hot_spot (text input)
- Chinese SSID Encoding:** UTF-8 (dropdown menu)
- * Security Mode:** WPA2 (dropdown menu)
- * RADIUS Server:** 192.168.0.200 (text input)
- * RADIUS Port:** 1812 (text input, Range: 1025 to 65535. Default: 1812)
- * RADIUS Key:** (password field)
- * Encryption Algorithm:** AES TKIP TKIP&AES
- Key Update Interval:** 0 (text input, Second, Range: 60 to 99999. 0 indicates no upgrade)

II. Configure the RADIUS server

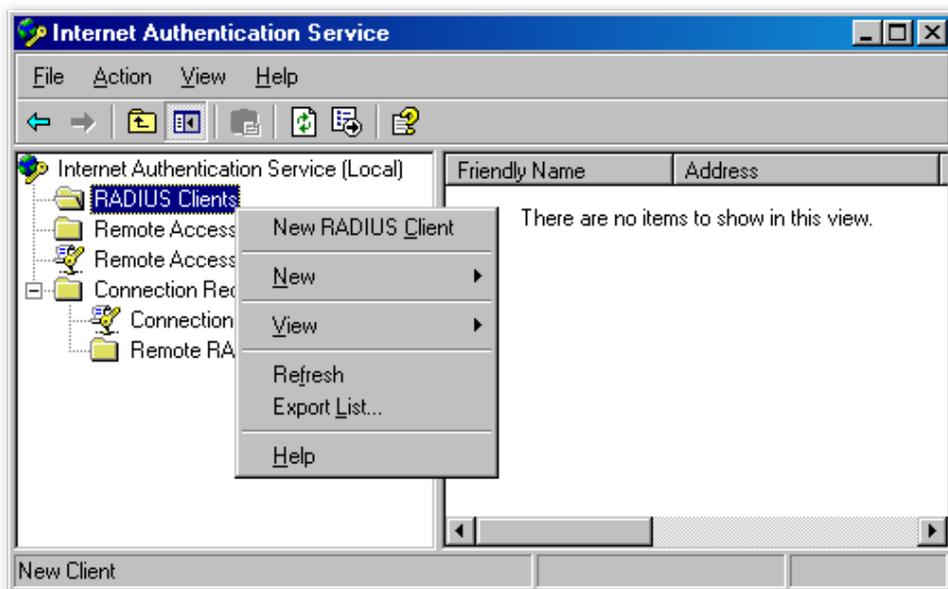


Tip

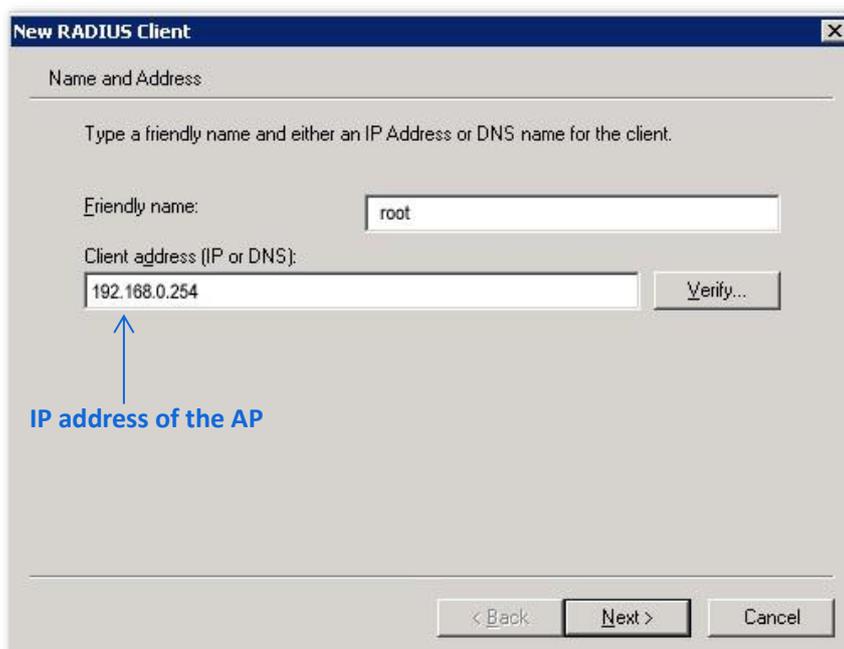
Windows 2003 is used as an example to describe how to configure the RADIUS server.

1. Configure a RADIUS client.

- (1) In the **Computer Management** dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.



- (2) Enter a RADIUS client name (which can be the name of the AP) and the IP address of the AP, and click **Next**.



- (3) Enter **qtW7J5cA** in the **Shared secret** and **Confirm shared secret** text boxes, and click **Finish**.

New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

Shared secret: xxxxxxxx

Confirm shared secret: xxxxxxxx

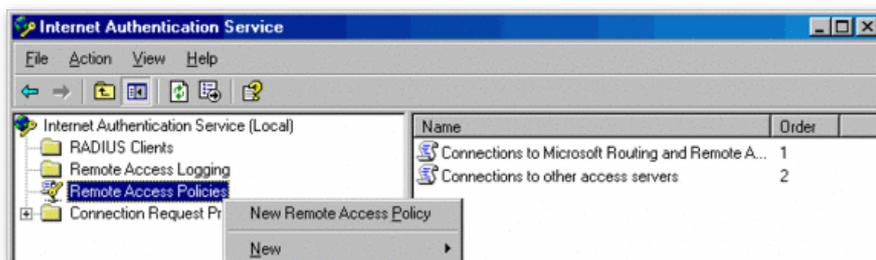
Request must contain the Message Authenticator attribute

Password same as that specified by RADIUS Password on the AP

< Back Finish Cancel

2. Configure a remote access policy.

- (1) Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



- (2) In the **New Remote Access Policy Wizard** dialog box that appears, click **Next**.

New Remote Access Policy Wizard

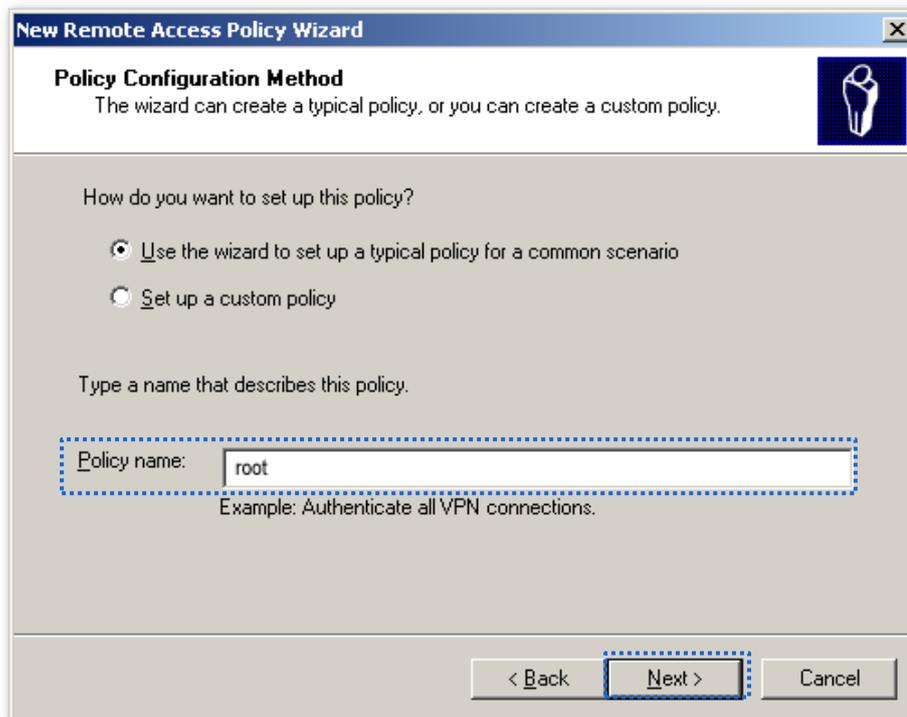
Welcome to the New Remote Access Policy Wizard

This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.

To continue, click Next.

< Back Next > Cancel

- (3) Enter a policy name and click **Next**.



New Remote Access Policy Wizard

Policy Configuration Method
The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

- Use the wizard to set up a typical policy for a common scenario
- Set up a custom policy

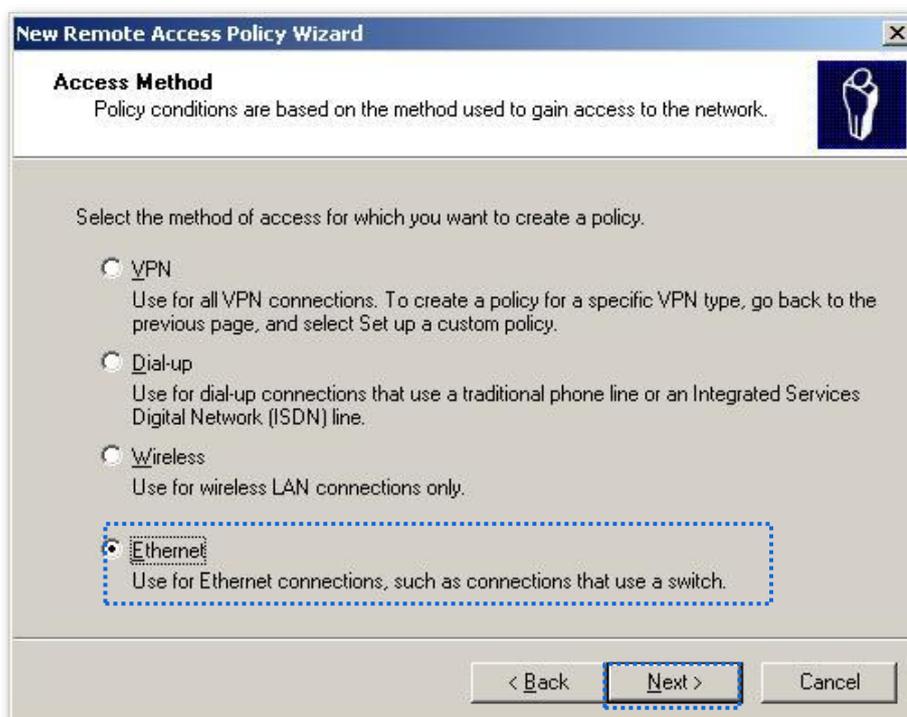
Type a name that describes this policy.

Policy name:

Example: Authenticate all VPN connections.

< Back **Next >** Cancel

- (4) Select **Ethernet** and click **Next**.



New Remote Access Policy Wizard

Access Method
Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

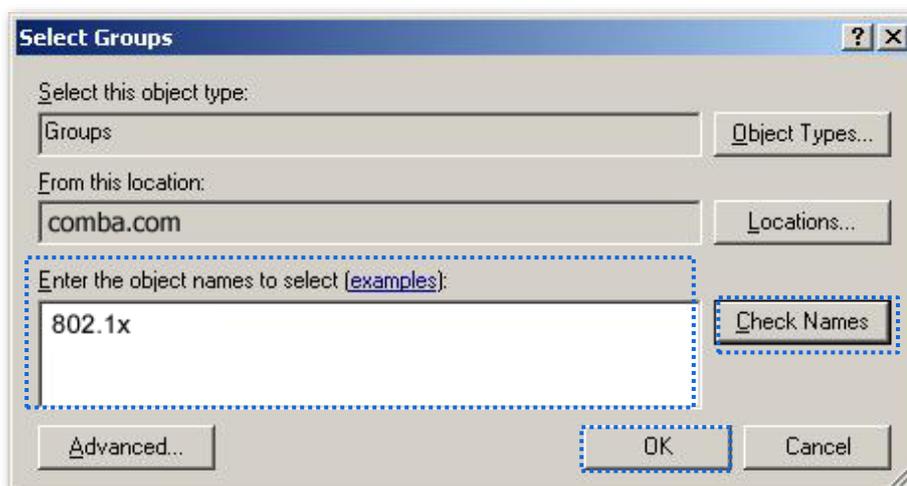
- VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
- Dial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
- Wireless
Use for wireless LAN connections only.
- Ethernet**
Use for Ethernet connections, such as connections that use a switch.

< Back **Next >** Cancel

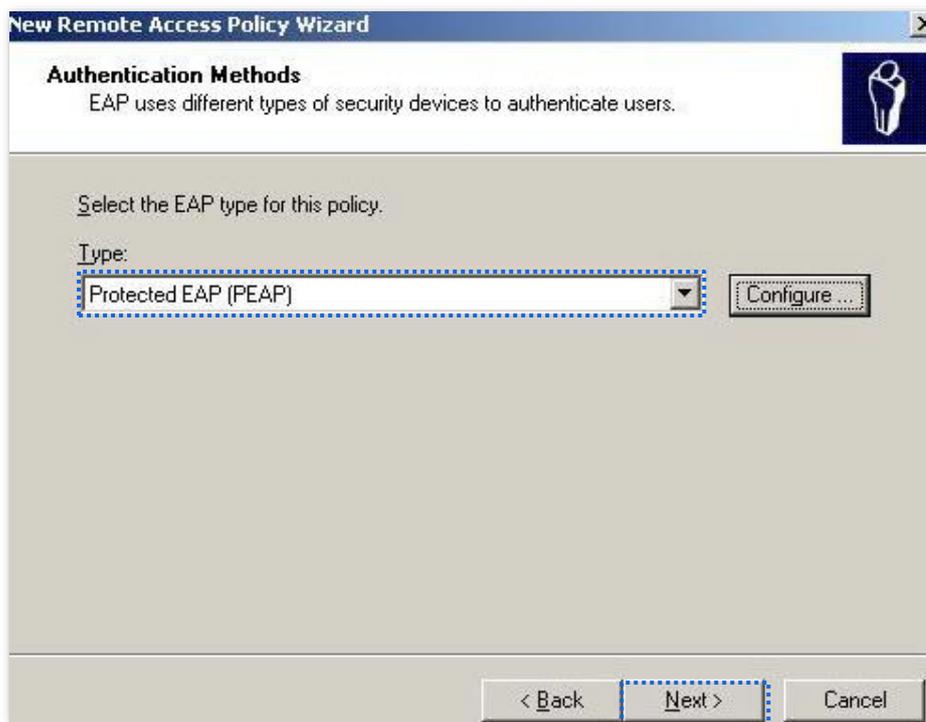
- (5) Select **Group** and click **Add**.



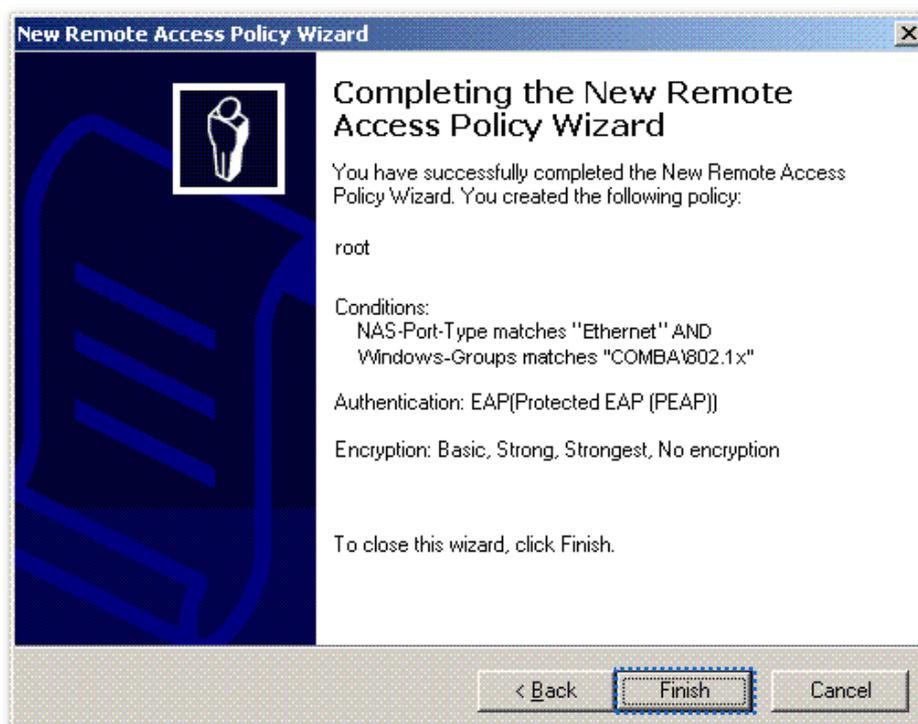
- (6) Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



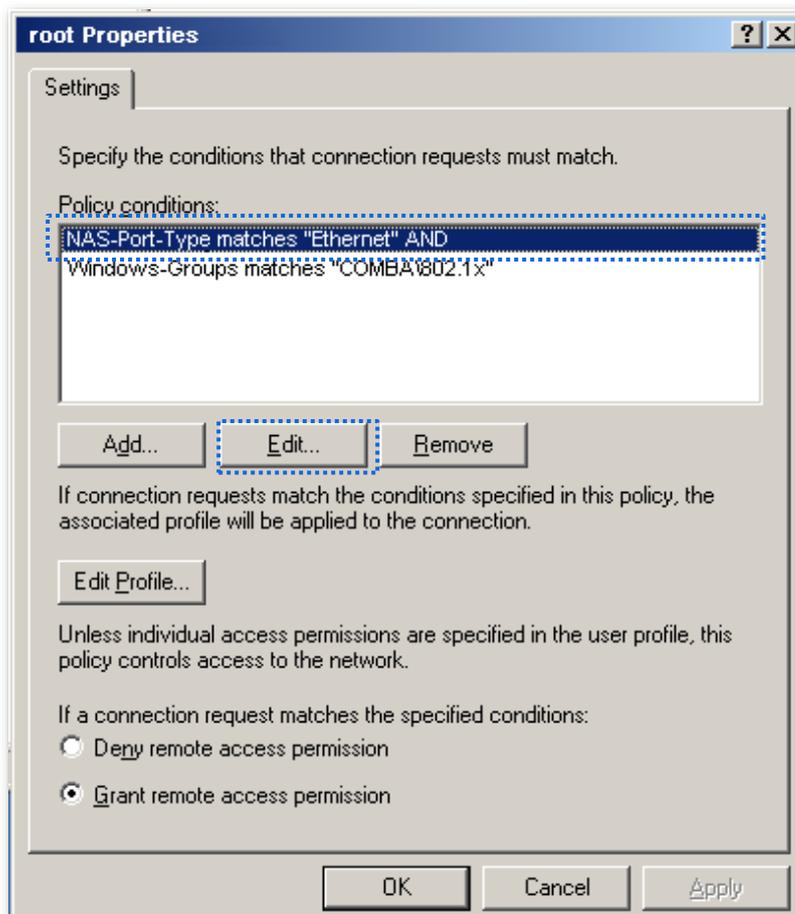
- (7) Select **Protected EAP (PEAP)** and click **Next**.



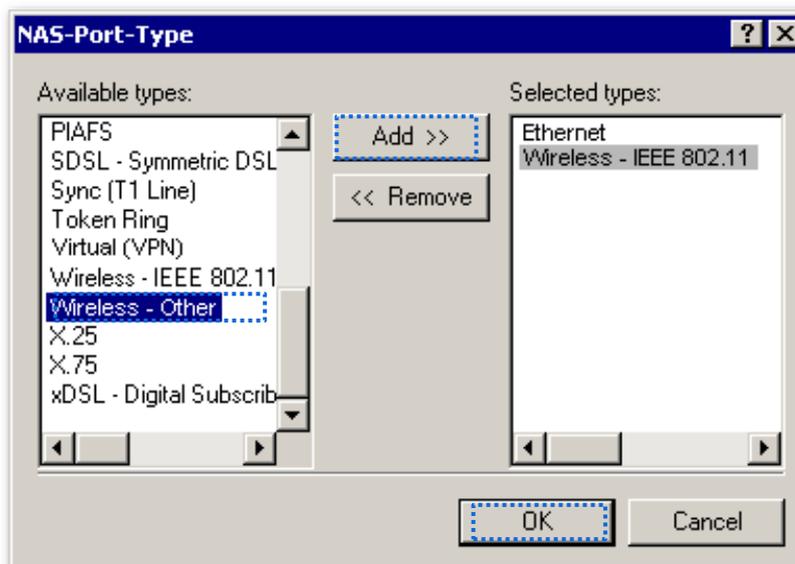
- (8) Click **Finish**. The remote access policy is created.



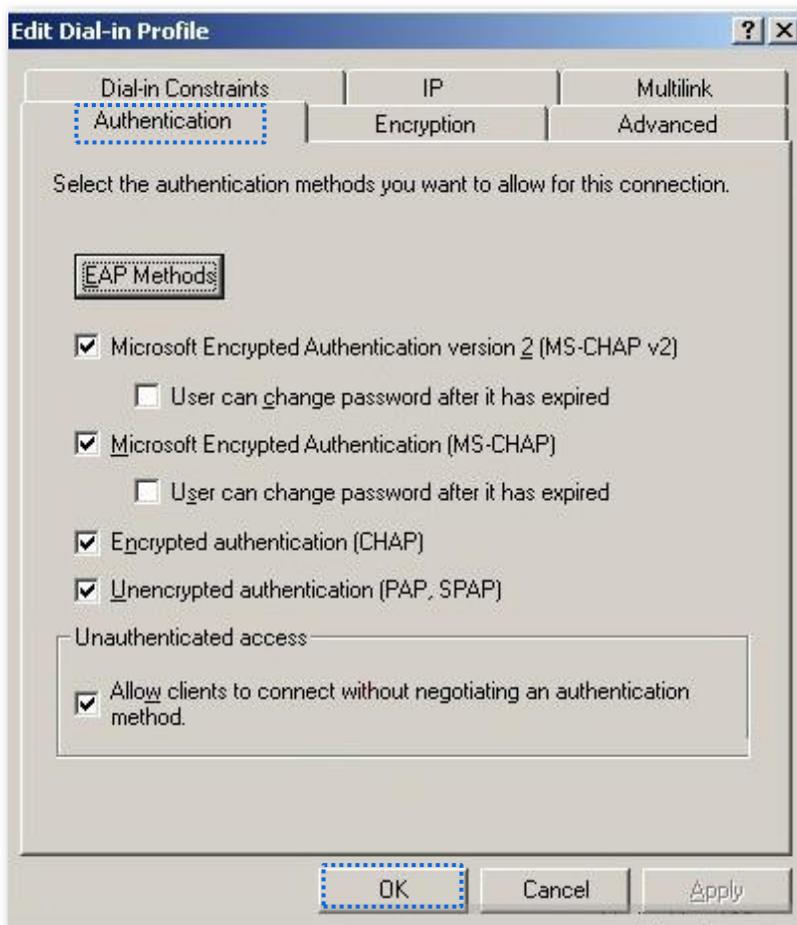
- (9) Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



- (10) Select **Wireless – Other**, click **Add**, and click **OK**.



- (11) Click **Edit Profile**, click the **Authentication** tab, configure settings as shown in the following figure, and click **OK**.



- (12) When a message appears, click **No**.

3. Configure user information.
Create a user and add the user to group **802.1x**.

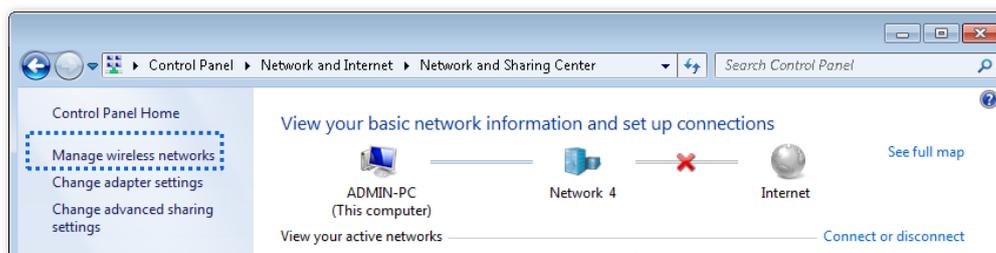
III. Configure your wireless device



Tip

Windows 7 is taken as an example to describe the procedure.

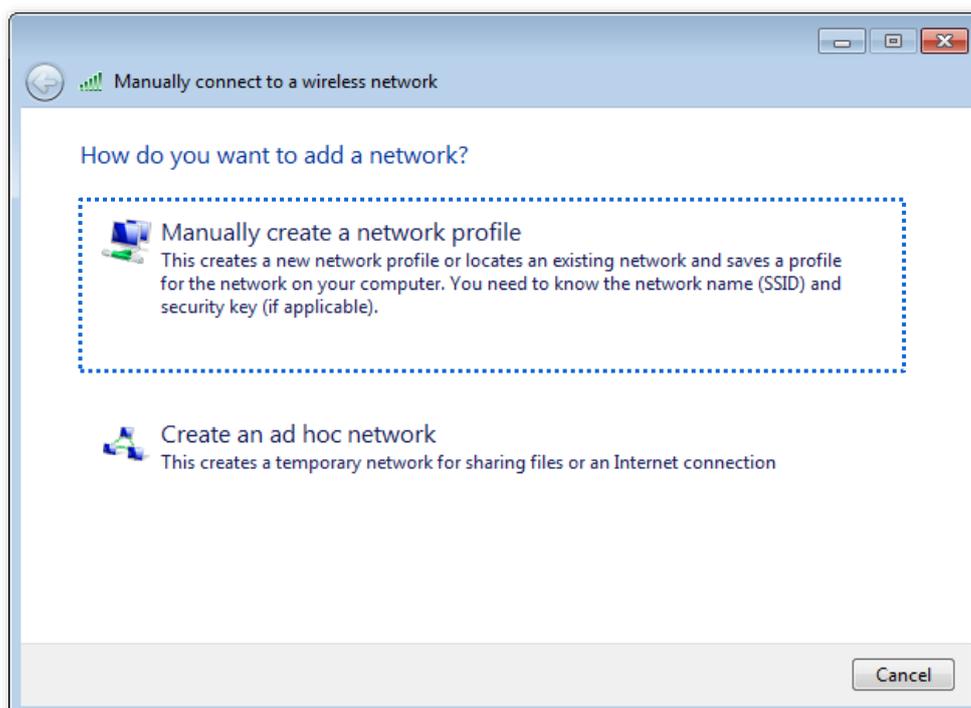
1. Choose **Start > Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



2. Click **Add**.



3. Click **Manually create a network profile**.



4. Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.

Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: hot_spot

Security type: WPA2-Enterprise

Encryption type: AES

Security Key: Hide characters

Start this connection automatically

Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

5. Click **Change connection settings**.

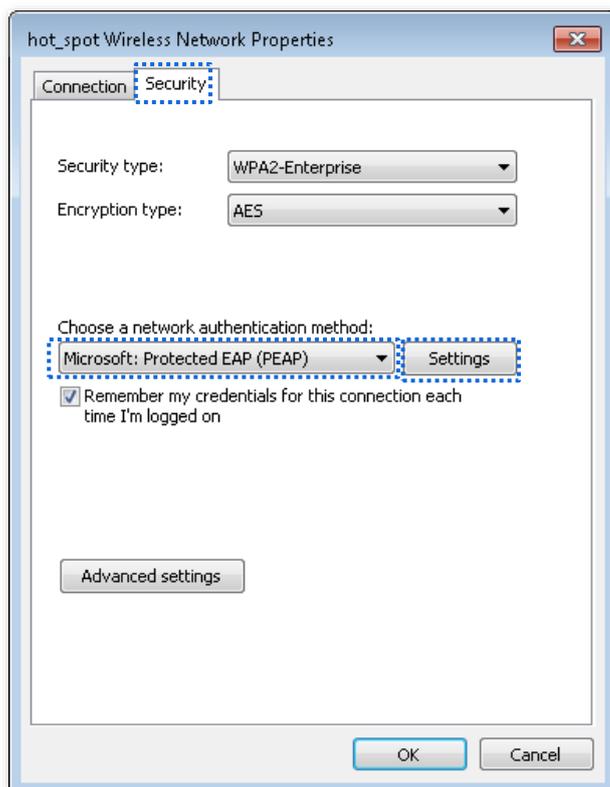
Manually connect to a wireless network

Successfully added hot_spot

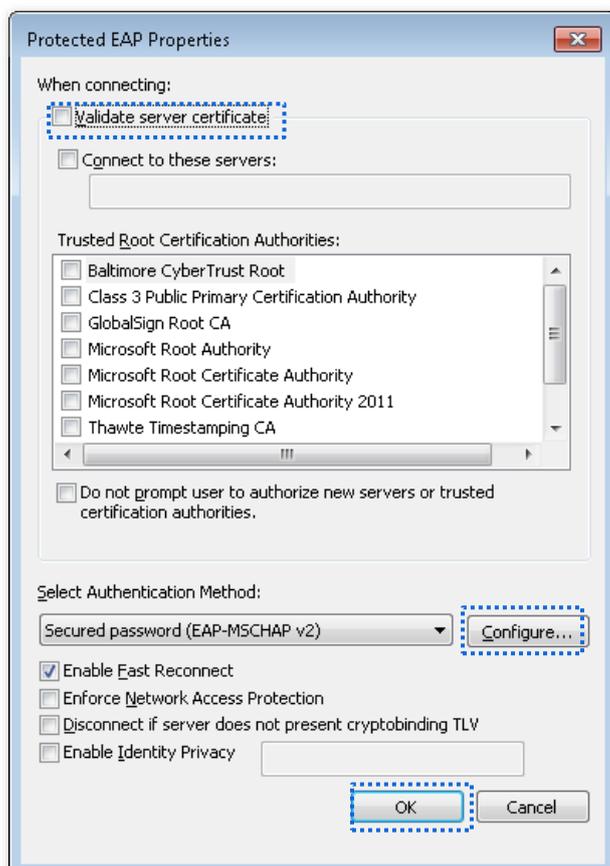
[Change connection settings](#)
Open the connection properties so that I can change the settings.

Close

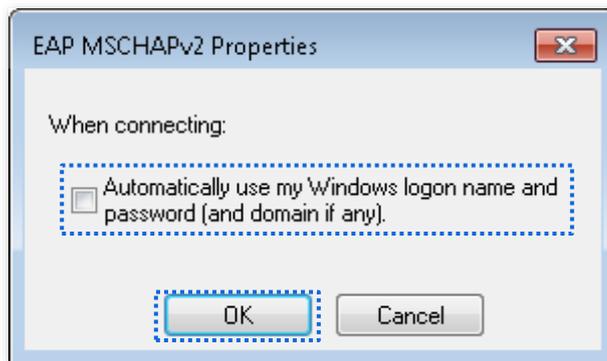
6. Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



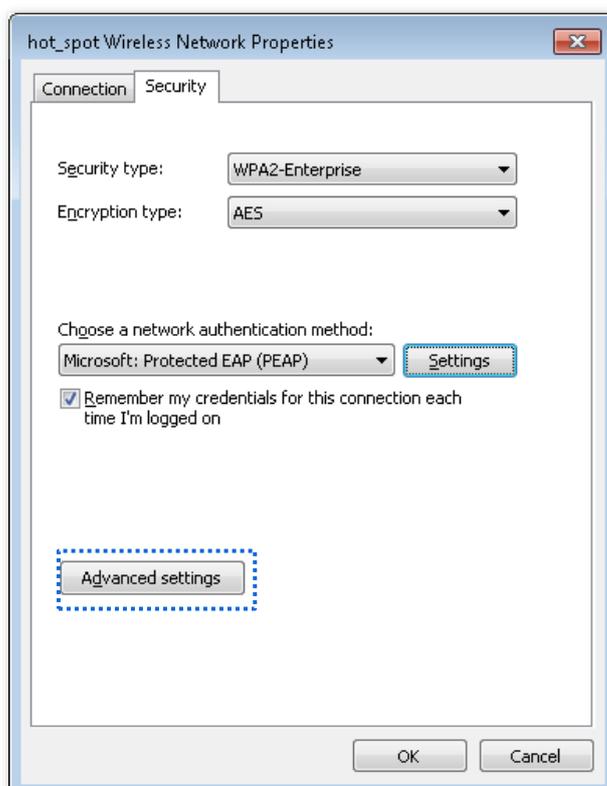
7. Deselect **Validate server certificate** and click **Configure**.



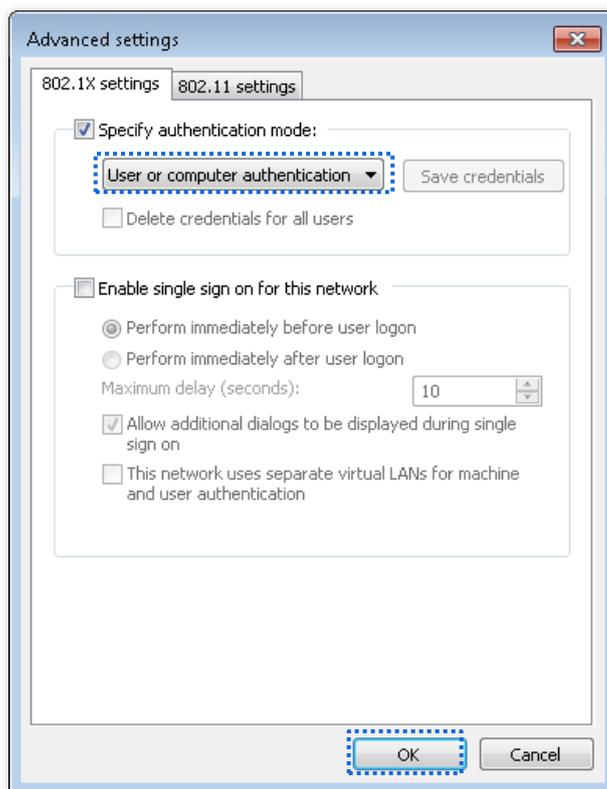
8. Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



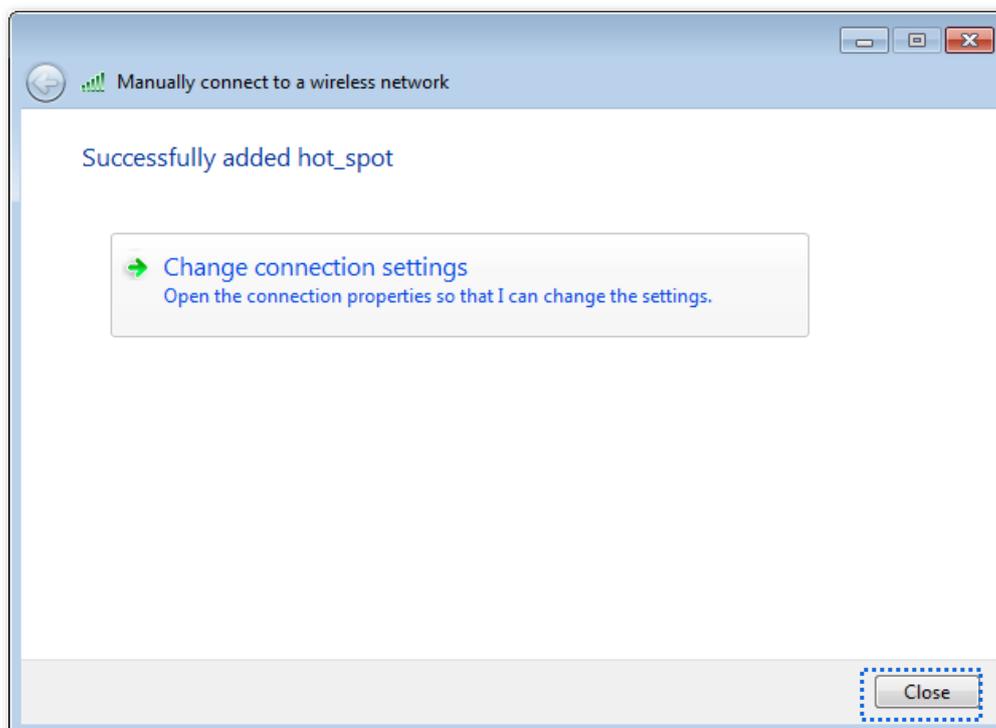
9. Click **Advanced settings**.

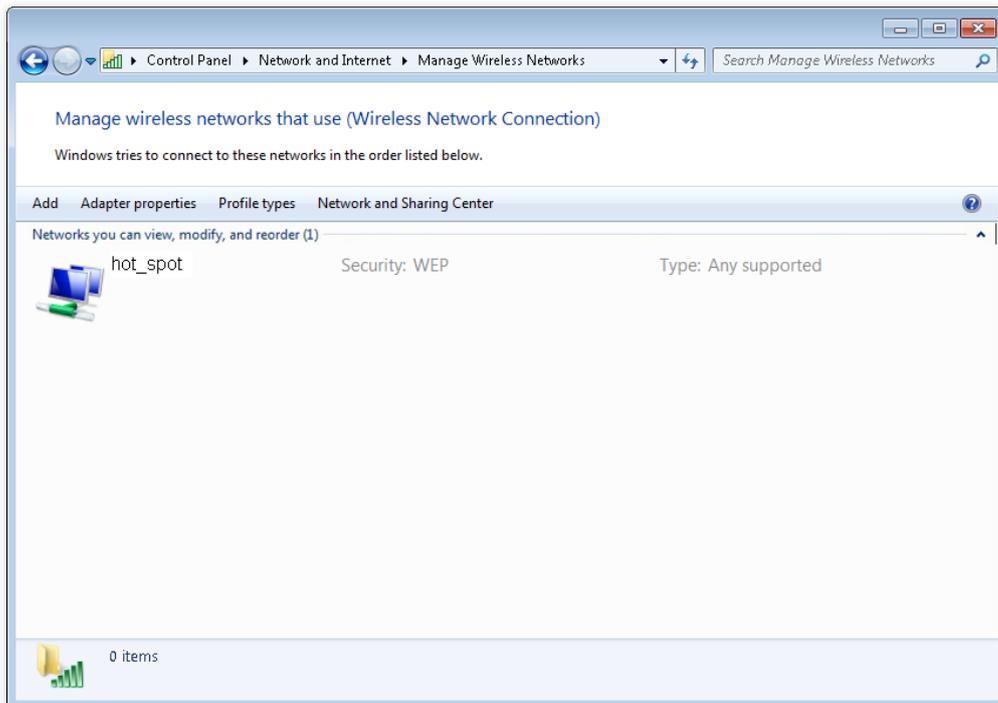


10. Select **User or computer authentication** and click **OK**.

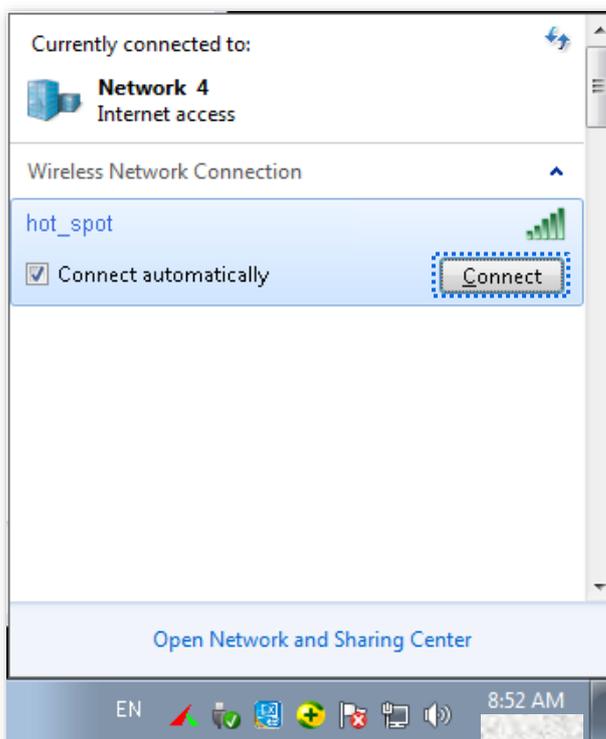


11. Click **Close**.

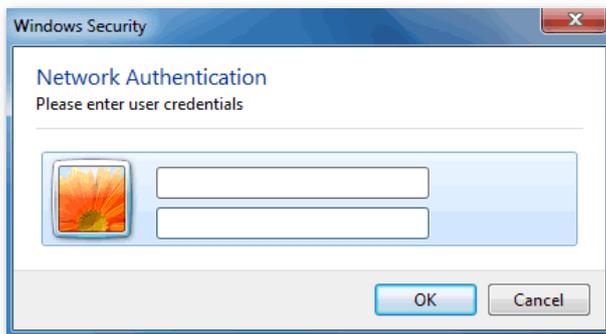




12. Click the network icon in the lower-right corner of the desktop and choose the wireless network of the AP, such as **hot_spot** in this example.



13. In the **Windows Security** dialog box that appears, enter the [user name and password](#) set on the RADIUS server and click **OK**.



---End

Verification

Wireless devices can connect to the wireless network named **hot_spot**.

6.2 RF Settings

To access the page, choose **Wireless > RF Settings**.

This page enables you to modify the basic radio parameters.

The screenshot displays the RF Settings interface for the 2.4 GHz band. At the top, there are tabs for '2.4 GHz' and '5 GHz'. A red help icon is visible in the top right corner. The settings are as follows:

- Wireless Network:
- Country/Region: China
- Network Mode: 11b/g/n/ax
- Channel: Auto
- Channel Bandwidth: 20/40MHz
- Extension Channel: Auto
- Lock Channel:
- Transmit Power: 21 dBm (range 13dBm to 21dBm)
- Lock Power:
- Preamble: Long Preamble Short Preamble
- Short GI: Enable Disable
- Suppress Broadcast Probe Response: Enable Disable

Parameter description

Parameter	Description
Wireless Network	It specifies whether to enable the wireless function of the AP.
Country/Region	It specifies the country or region where the AP is used. This parameter helps comply with channel regulations of the country or region. This parameter can be set if Lock Channel is not selected.
Network Mode	<p>It specifies the wireless network mode of the AP. This parameter can be set if Lock Channel is not selected.</p> <p>Available options for 2.4 GHz are 11b, 11g, 11b/g, 11b/g/n and 11b/g/n/ax.</p> <ul style="list-style-type: none"> – 11b: The AP works in 802.11b mode and only wireless devices compliant with 802.11b can connect to the 2.4 GHz wireless networks of the AP. – 11g: The AP works in 802.11g mode and only wireless devices compliant with 802.11g can connect to the 2.4 GHz wireless networks of the AP. – 11b/g: The AP works in 802.11b/g mode and only wireless devices compliant with 802.11b or 802.11g can connect to the 2.4 GHz wireless networks of the AP. – 11b/g/n: The AP works in 802.11b/g/n mode. Wireless devices compliant with 802.11b or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n can connect to the 2.4 GHz wireless networks of the AP. – 11b/g/n/ax: The AP works in 11b/g/n/ax mode. Wireless devices compliant with 802.11b, or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n or 802.11ax can connect to the 2.4 GHz wireless networks of the AP. <p>Available options for 5 GHz are 11a, 11a/n, 11ac and 11a/n/ac/ax.</p> <ul style="list-style-type: none"> – 11a: The AP works in 802.11a mode and only wireless devices compliant with 802.11a can connect to the 5 GHz wireless networks of the AP. – 11a/n: The AP works in 802.11a/n mode and only wireless devices compliant with 802.11a or 802.11n can connect to the 5 GHz wireless networks of the AP. – 11ac: The AP works in 802.11ac mode and only wireless devices compliant with 802.11ac can connect to the 5 GHz wireless networks of the AP. – 11a/n/ac/ax: The AP works in 11a/n/ac/ax mode. Wireless devices compliant with 802.11a, or 802.11ac and wireless devices working at 5 GHz and compliant with 802.11n or 802.11ax can connect to the 5 GHz wireless networks of the AP.
Channel	<p>It specifies the operating channel of the AP. This parameter can be set if Lock Channel is not selected.</p> <p>Auto: It indicates that the AP automatically adjusts its operating channel according to the ambient environment.</p>

Parameter	Description
Channel Bandwidth	<p>It specifies the wireless channel bandwidth of the AP. This parameter can be set if the AP works in 11 b/g/n, 11ac, 11a/n mode and Lock Channel is not selected.</p> <ul style="list-style-type: none"> – 20MHz: It indicates that the AP can use only 20 MHz channel bandwidth. – 40MHz: It indicates that the AP can use only 40 MHz channel bandwidth. – 20/40MHz: It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment. – 80MHz: Only available for 5 GHz. It indicates that the AP can use only 80 MHz channel bandwidth. – 160MHz: Only available for 5 GHz. It indicates that the AP can use only 160 MHz channel bandwidth. – 20/40/80/160MHz: Only available for 5 GHz. It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz, 40 MHz, 80 MHz, or 160 MHz according to the ambient environment.
Extension Channel	It is used to determine the operating frequency band of this device when it uses the 40 MHz channel bandwidth in 11n mode.
Lock Channel	It is used to lock the channel settings of the AP. If this parameter is selected, channel settings including Country/Region , Network Mode , Channel , Channel Bandwidth , and Expansion Channel cannot be changed.
Transmit Power	<p>It specifies the transmit power of the AP.</p> <p>A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the wireless network performance and security.</p>
Lock Power	It specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.
Preamble	<p>A preamble is a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data.</p> <p>By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the Short Preamble option.</p>
Short GI	<p>Short Guard Interval.</p> <p>There is a delay on the receiving side due to multipath and other factors during the wireless signal transmission in space. If the subsequent data block is transmitted too quickly, it will interfere with the previous data block, and the short guard interval can be used to circumvent this interference. Short GI helps to increase the wireless throughput by 10%.</p>
Suppress Broadcast Probe Response	<p>By default, wireless devices keep sending Probe Request packets that include the SSID field to scan their nearby wireless networks. After receiving such packets, this device determines whether the wireless devices are allowed to access its wireless networks based on the packets and responds using the Probe Response packets (including all Beacon frame parameters), which consumes a lot of wireless resources.</p> <p>After this function is enabled, this device does not respond to the requests without an SSID, saving wireless resources.</p>

6.3 RF Optimization

To access the page, choose **Wireless > RF Optimization**.

This page enables you to modify the radio parameters to optimize performance.



You are strongly recommended to modify the settings only with professional guidance to prevent degrading wireless performance.

2.4 GHz 5 GHz
?

Beacon Interval ms (Range: 20 to 999. Default: 100)

Fragment Threshold (Range: 256 to 2346. Default: 2346)

RTS Threshold (Range: 1 to 2347. Default: 2347)

DTIM Interval (Range: 1 to 255. Default: 1)

RSSI Threshold dBm (Range: -90 to -60. Default: -90)

Signal Transmission Coverage-oriented Capacity-oriented

Air Interface Scheduling Enable Disable

Anti-interference Mode (Range: 0 to 3. Default: 3)

APSD Enable Disable

MU-MIMO Enable Disable

OFDMA Enable Disable

Client Timeout Interval

Mandatory Rate 1 2 5.5 6 9 11 12 18 24 36 48 54 All

Optional Rate 1 2 5.5 6 9 11 12 18 24 36 48 54 All

Save
Cancel

Parameter description

Parameter	Description
Beacon Interval	<p>Used to set the interval at which this device sends Beacon frames.</p> <p>Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.</p>
Fragment Threshold	<p>Threshold of a fragment.</p> <p>Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented.</p> <p>In case of a high error rate, you can reduce the threshold to enable this device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput.</p> <p>In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput.</p>
RTS Threshold	<p>Frame length threshold for triggering the RTS/CTS mechanism. The unit is byte.</p> <p>If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts.</p> <p>Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold to reduce conflicts.</p> <p>The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.</p>
DTIM Interval	<p>Countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval.</p> <p>A countdown starts from this value. The AP transmits broadcast and multicast frames in its cache only when the countdown reaches zero.</p> <p>For example, if DTIM Interval is set to 1, this device transmits all cached frames at one Beacon interval.</p>
RSSI Threshold	<p>It specifies the minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device.</p> <p>A proper value facilitates wireless devices to connect to the AP with stronger signal in case of multiple APs exist.</p>
Signal Transmission	<p>Select the option based on your actual situation.</p> <ul style="list-style-type: none"> – Coverage-oriented: This mode broadens WiFi coverage of APs, and is usually used in scenarios deployed with fewer APs, such as offices, warehouses, and hospitals. – Capacity-oriented: This mode effectively decreases mutual interference among APs, and is usually used in scenarios deployed with massive APs, such as conferences, exhibition halls, banquet halls, stadiums, classrooms of higher-education institutes, airports and so on.
Prioritize 5 GHz	<p>Enable: It specifies that dual band wireless devices prefer the 5 GHz WiFi network of the AP to connect.</p>

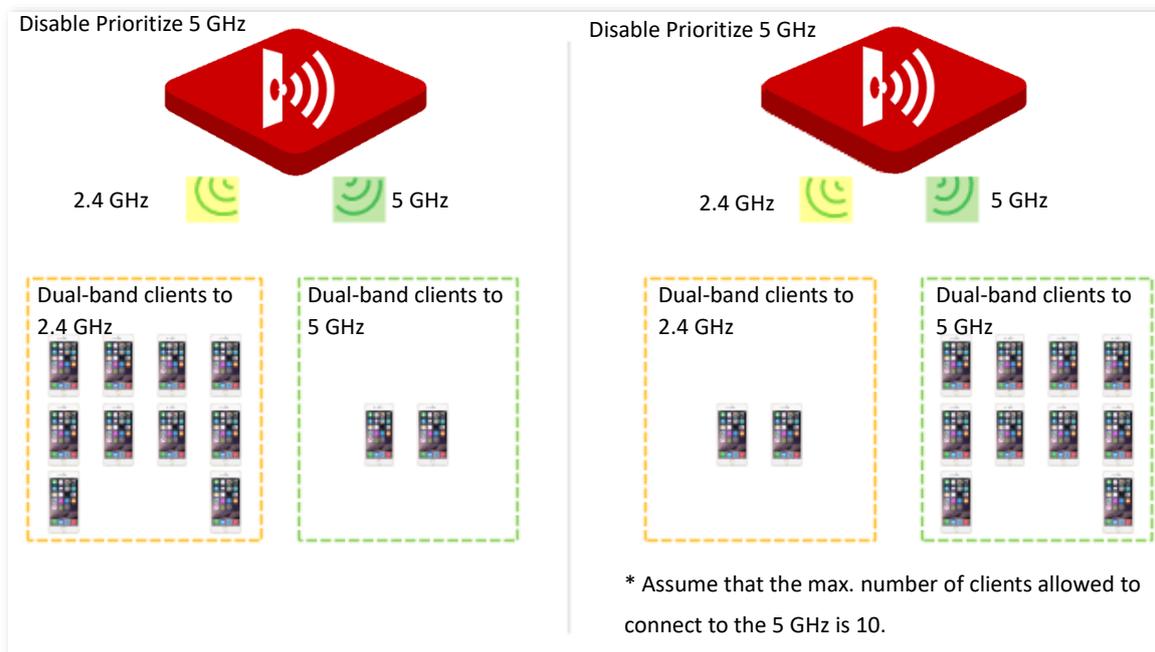
Parameter	Description
Prioritize 5 GHz Threshold	With this function enabled, if the strength of the signals transmitted by a wireless device is stronger than this threshold, the wireless device connects to the 5 GHz WiFi network. Otherwise, it connects to the 2.4 GHz WiFi network.
Air Interface Scheduling	If this function is enabled, the same download time is assigned to users experiencing different download rates, ensuring a better experience for high-rate users.
Anti-interference Mode	Interference mitigation mode of this device. The default option is 3 (Suppress critical interference) . <ul style="list-style-type: none"> – 0 (Disable): Interference suppression measures are disabled. – 1 (Suppress weak interference): Suppress mild interference for weak radio environment. – 2 (Suppress moderate interference): Suppress moderate interference for bad radio environment. – 3 (Suppress critical interference): Suppress critical interference for heavy loading radio environment.
APSD	Automatic Power Save Delivery. APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
MU-MIMO	Multi-User Multiple-Input Multiple-Output. If enabled, AP can communicate with multiple users concurrently, avoiding WiFi network congestion and improving communication.
OFDMA	Orthogonal Frequency Division Multiple Access. If this function is enabled, multiple clients can transmit data at the same time, so that the transmission efficiency is improved, delay is reduced, and user experience is enhanced.
Client Timeout Interval	Used to set the wireless client disconnection interval of this device. The device disconnects from a wireless client if no traffic is transmitted or received by the wireless client within the interval.
Mandatory Rate	It specifies rates that wireless clients must support to connect to the wireless networks of this device.
Optional Rate	It specifies the additional rates that the AP supports, which are optional to wireless clients.

■ Prioritize 5 GHz

Although the 2.4 GHz band is more widely used than the 5 GHz band in actual wireless networks application, channels and signals on 2.4 GHz suffer more serious congestion and interference since there are only 3 non-overlapped communication channels on this band. The 5 GHz band could provide more non-overlapped communication channels. The quantity could reach more than 20 in some countries.

With the evolvement of the wireless networks, wireless clients that support both the 2.4 GHz and 5 GHz are more popular. However, by default, such dual-band wireless clients choose the 2.4 GHz to connect, resulting in even worse congestion of the 2.4 GHz band and the waste of the 5 GHz band.

The Prioritize 5 GHz function enables such dual-band wireless clients to connect the 5 GHz band on network initialization if the 5 GHz signal strength the AP received reaches or exceeds the 5 GHz threshold so as to improve the utilization of the 5 GHz band, reduce the load and interference on the 2.4 GHz band, thus bettering user experience.



Note

The prioritize 5 GHz function takes effect only on the condition that both the 2.4 GHz and 5 GHz wireless networks are enabled, and the two bands share the same SSID, security mode and password.

■ Air Interface Scheduling

In mixed wireless rates environment, the traditional First-in First-out (FIFO) allocates more air interface time to clients with low transmission capacity and low spectrum efficiency, reducing the system throughput of each AP then the system utilization.

The air interface scheduling function evenly allocates downlink transmission time to clients so that clients with high transmission rate could transmit more data, improving the throughput of each AP and number of clients allowed to be connected.

6.4 Frequency Analysis

6.4.1 Overview

To access the page, choose **Wireless > Frequency Analysis**.

This page allows you to analyze frequency and scan channels.

- **Frequency Analysis**

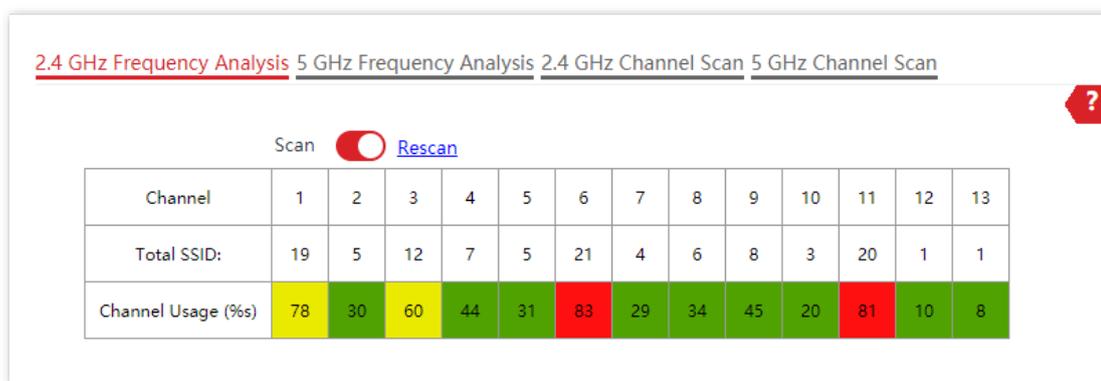
From the intuitive result, you can check how many wireless networks (total SSIDs) use the same channel and choose a channel with low usage as the operating channel of the device for better wireless transmission efficiency.

- **Channel Scan**

The scan result list presents you with information about nearby wireless network, including SSID, MAC address, channel, channel bandwidth, and signal strength.

6.4.2 View Frequency Analysis

1. Choose **Wireless > Frequency Analysis**.
2. Click **2.4 GHz Frequency Analysis** or **5 GHz Frequency Analysis** tab to select the wireless network radio band for frequency analysis. **2.4 GHz Frequency Analysis** is taken as an example here.
3. Enable **Scan**.



---End

After scanning, you can select a channel with low usage as the AP operating channel.

- ■: High channel usage. The channel is not recommended.
- ■: Moderate channel usage.
- ■: Low channel usage. The channel is recommended.

6.4.3 Execute Channel Scan

1. Choose **Wireless > Frequency Analysis**.
2. Click **2.4 GHz Channel Scan** or **5 GHz Channel Scan** tab to select the wireless network radio band for channel scan. **2.4 GHz Channel Scan** is taken as an example here.
3. Enable **Scan**.

2.4 GHz Frequency Analysis 5 GHz Frequency Analysis 2.4 GHz Channel Scan 5 GHz Channel Scan

Scan Rescan

ID	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
1	NOVA_MUY2_A3	C8:3A:35:9A:3B:5A	20	10	WPA2-PSK,AES	
2	EW15D	D8:38:0D:EE:11:71	20	6	WPA2-PSK,AES	

---End

6.5 WMM

6.5.1 Overview

802.11 networks offer wireless access services based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) channel competition mechanism, which allows all wireless clients to fairly compete for channels. All the services implemented over wireless networks share the same channel competition parameters. Nevertheless, different services usually have different requirements for bandwidth, delay, and jitter. This requires wireless networks to offer accessibility based on the services implemented over the networks.

WMM is a wireless QoS protocol used to ensure that packets with high priorities are transmitted first. This ensures better voice and video service experience over wireless networks.

WMM involves the following terms:

- Enhanced Distributed Channel Access (EDCA): It is a channel competition mechanism to ensure that packets with higher priorities are assigned more bandwidth and transmitted earlier.
- Access Category (AC): The WMM mechanism divides WLAN traffic by priority in descending order into the AC-VO (voice stream), AC-VI (video stream), AC-BE (best effort), and AC-BK (background) access categories. The access categories use queues with different priorities to send packets. The WMM mechanism ensures that packets in queues with higher priorities have more opportunities to access channels.

According to the 802.11 protocol family, all devices listen on a channel before using the channel to send data. If the channel stays idle for a specified period or longer, the devices wait a random backoff period within the contention window. The device whose backoff period expires first can use the channel. The 802.11 protocol family applies the same backoff period and contention window to all devices across a network to ensure that the devices have the same channel contention opportunity.

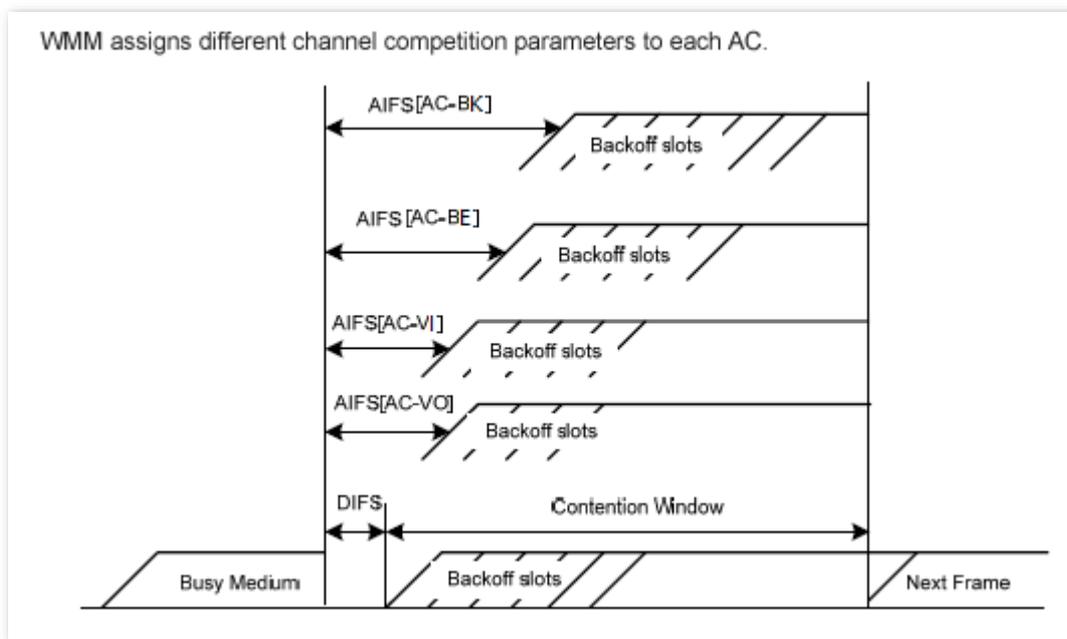
■ EDCA Parameters

WMM changes the contention mechanism of 802.11 networks by dividing packets into four ACs, among which the ACs with higher priorities have more opportunities to access channels. The ACs help achieve different service levels.

WMM assigns each AC a set of EDCA parameters for channel contention, including:

- Arbitration Inter Frame Spacing Number (AIFSN): Different from the fixed distributed inter-frame spacing (DIFS) specified in the 802.11 protocol family, AIFSN varies across ACs. A greater AIFSN indicates a longer backoff period. See AIFS in the following figure.

- Contention window minimum (CW_{min}) and contention window maximum (CW_{max}) specify the average backoff period. The period increases along with these two values. See the backoff slots in the following figure.
- Transmission Opportunity (TXOP): It specifies the maximum channel use duration after successful channel contention. The duration increases along with this value. The value **0** indicates that a device can send only one packet through a channel after winning contention for the channel.



■ ACK Policies

WMM specifies the Normal ACK and No ACK policies.

- According to the No ACK policy, no ACK packet is used during wireless packet transmission to acknowledge packet reception. This policy is applicable to scenarios where interference is mild and can effectively improve transmission efficiency. In case of strong interference, lost packets will not be resent if this policy is adopted. This leads to a higher packet loss rate and reduces the overall performance.
- According to the Normal ACK policy, each time a receiver receives a packet, it sends back an ACK packet to acknowledge packet reception.

6.5.2 Configure WMM settings

1. Choose **Wireless > Access Control**.
2. Select a wireless network radio band on which access control is to be implemented.
3. Select a WMM optimization mode as required.
4. Change the parameters as required when the optimization mode is set to **Custom**.
5. Click **Save**.

2.4 GHz 5 GHz ?

WMM Optimization Optimized for scenario with 1 - 10 users
 Optimized for scenario with more than 10 users
 Custom

No ACK

EDCA AP Parameter

	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="3"/>	<input type="text" value="0"/>
AC_BK	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="1"/>	<input type="text" value="94"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="1"/>	<input type="text" value="47"/>

EDCA STA Parameter

	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="3"/>	<input type="text" value="0"/>
AC_BK	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="94"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="47"/>

Parameter description

Parameter	Description
WMM Optimization	<p>It specifies the WMM optimization modes supported by the AP:</p> <ul style="list-style-type: none"> - Optimized for scenario with 1 - 10 users: If 10 or less clients are connected to the AP, you are recommended to select this mode to obtain higher client throughput. - Optimized for scenario with more than 10 users: If more than 10 clients are connected to the AP, you are recommended to select this mode to ensure client connectivity. - Custom: This mode enables you to set the WMM EDCA parameters for manual optimization.
No ACK	<ul style="list-style-type: none"> - If the check box is selected, the No ACK policy is adopted. - If the check box is deselected, the Normal ACK policy is adopted.
EDCA AP Parameters	For details, refer to section 6.5.1 Overview .
EDCA STA Parameters	

6.6 Access Control

6.6.1 Overview

The access control function enables you to allow or disallow the wireless devices to access the wireless network of the AP based on their MAC addresses.

To access the page, choose **Wireless > Access Control**.

The AP supports the following two filter modes:

- **Whitelist:** It indicates that only the wireless devices with the specified MAC addresses can access the wireless networks of the AP.
- **Blacklist:** It indicates that only the wireless devices with the specified MAC addresses cannot access the wireless networks of the AP.

6.6.2 Configure Access Control

1. Choose **Wireless > Access Control**. Select a wireless network radio band on which access control is to be implemented.
2. From the **SSID** drop-down list box, select an SSID of the wireless network to which the rule applies.
3. Enable **Access Control**.
4. Set **Mode** to **Blacklist** or **Whitelist**.
5. Enter the MAC address of the wireless device to which the rule applies. Then click **Add**.



If the wireless device to be controlled has connected to the AP, click **Add Online Devices** to quickly add the MAC address of the device to the access control client list.

6. Click **Save**.

2.4 GHz 5 GHz

SSID

Access Control

Mode Blacklist Whitelist

MAC Address

ID	MAC Address	Status	Operation
No data			

---End

Parameter description

Parameter	Description
SSID	It specifies the wireless network to which the rule applies.
Access Control	It specifies whether to enable or disable the wireless control function.
Mode	It specifies the access control mode <ul style="list-style-type: none"> – Blacklist: It indicates that only the wireless clients on the wireless access control list cannot connect to the AP with the selected SSID. – Whitelist: It indicates that only the wireless clients on the wireless access control list can connect to the AP with the selected SSID.

6.6.3 Example of Configuring Access Control

Networking requirement

A wireless network whose SSID is **VIP** under the 5 GHz radio band has been set up in a company. Only a few members are allowed to connect to the wireless network.

The Access Control function of the AP is recommended. The members have three wireless devices whose MAC addresses are **D8:38:0D:00:00:01**, **D8:38:0D:00:00:02**, and **D8:38:0D:00:00:03**.

Configuration procedure

1. Choose **Wireless > Access Control > 5 GHz**.
2. Select **VIP** from the **SSID** drop-down list.
3. Enable **Access Control**.
4. Set **Mode** to **Whitelist**.
5. Enter **D8:38:0D:00:00:01** in the **MAC Address** text box and click **Add**.
6. Repeat step [5](#) to add **D8:38:0D:00:00:02** and **D8:38:0D:00:00:03** as well.
7. Click **Save**.

---End

The following figure shows the configuration.

The screenshot shows the configuration page for the 5 GHz wireless network. The SSID is set to 'VIP'. Access Control is enabled. The Mode is set to 'Whitelist'. Below the mode selection, there is a MAC Address input field with a format hint 'Format: XX:XX:XX:XX:XX:XX' and 'Add' and 'Add Online Devices' buttons. A table below shows the configured MAC addresses and their status.

ID	MAC Address	Status	Operation
1	D8:38:0D:00:00:01	Enable	
2	D8:38:0D:00:00:02	Enable	
3	D8:38:0D:00:00:03	Enable	

At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons.

Verification

Only the specified wireless devices can connect to the **VIP** wireless network.

6.7 Advanced Settings

6.7.1 Overview

This page enables you to set the **Identify Client Type** and **Broadcast Packet Filter** of the AP.

To access the page, choose **Wireless > Advanced Settings**.

- **Identify Client Type**

It specifies whether to identify operating system types of wireless clients connected to this device. Terminal types that the AP can identify include: Android, iOS, WPhone, Windows, Mac OS.

- **Broadcast Packet Filter**

By default, this device forwards lots of invalid broadcast packets from wired networks, which may affect business data transfer. The broadcast packet filter function allows you to filter broadcast packets by types so that invalid packets are not forwarded. This reduces air interface resources usage and ensures more bandwidth for business data transfer.

6.7.2 Configure Advanced Settings

1. Choose **Wireless > Advanced Settings**
2. Change the parameters as required.
3. Click **Save**.

Advanced Settings

Identify Client Type Enable Disable

Broadcast Packet Filter Enable Disable

Filters

Save Cancel

---End

Parameter description

Parameter	Description
Identify Client Type	If this function is enabled and the client connected to the AP has accessed an http:// URL , the operating system type of the client can be viewed by choosing Status > Client List .
Broadcast Packet Filter	If this function is enabled, the AP can reduce air interface resources usage and ensure the bandwidth for business data transfer.
Filters	Select a mode after you enable the Broadcast Packet Filter function. <ul style="list-style-type: none"> – Excludes DHCP and ARP: Filter out all broadcast or multicast data except DHCP and ARP packets. – Excludes ARP: Filter out all broadcast or multicast data except ARP packets.

6.8 QVLAN Settings

6.8.1 Overview

The AP supports 802.1Q VLANs and is applicable in a network environment where 802.1Q VLANs have been defined. By default, the QVLAN function is disabled.

If the QVLAN function is enabled, tagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the VID in the data, whereas untagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the PVID of the port that receives the data.

The following table describes how ports of different link types process transmitted and received data.

Port	Method to Process Received Data		Method to Process Transmitted Data
	Tagged Data	Untagged Data	
Access	Forward the data to other ports of the VLAN corresponding to the VID in the data.	Forward the data to the other ports of the VLAN corresponding to the PVID of the port that receives the data.	Transmit data after removing tags from the data.
Trunk			Transmit data without removing tags from the data.

6.8.2 Configure the QVLAN Function

1. Choose **Wireless > QVLAN Settings**.
2. Enable QVLAN Settings.
3. Change the parameters as required. Generally, you only need to change the **2.4 GHz SSID VLAN ID** and **5 GHz SSID VLAN ID** settings.
4. Click **Save**.

QVLAN Settings

*Enable

QVLAN Mode: QVLAN

PVID: 1

Management VLAN: 1

Trunk Port: LAN0 LAN1

Wired LAN Port VLAN ID (1 to 4094)

LAN0: 1

LAN1: 1

*2.4 GHz SSID VLAN ID (1 to 4094)

IP-COM_81AAE1: 1000

*5 GHz SSID VLAN ID (1 to 4094)

VIP: 1000

Save Cancel

---End

Parameter description

Parameter	Description
Enable	It specifies whether to enable the QVLAN function of the AP. By default, it is disabled.

Parameter	Description
QVLAN Mode	<p>It specifies the QVLAN mode of the AP.</p> <ul style="list-style-type: none"> – QVLAN: Enable the 802.1Q VLAN function of the AP. – IPTV: It is used in IPTV business scenarios. This function needs to be used with the IPTV function of an IP-COM enterprise router of the same brand. It can establish an IPTV data transparent transmission channel between the router and the AP, and solve the problem of difficult connection caused by the long distance between the IPTV set-top box and the optical modem. In this mode, you need to bind the AP to the network port of the IPTV set-top box on the router.
PVID	It specifies the ID of the default native VLAN of the trunk port of the AP.
Management VLAN	<p>It specifies the ID of the AP management VLAN.</p> <p>After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.</p>
Trunk Port	<p>It specifies the LAN port used as a trunk port of the AP. The default value is LAN0. Traffic of all VLANs can pass through a trunk port.</p> <p> Note</p> <p>If the QVLAN function is enabled, at least one LAN port needs to be set as a trunk port.</p>
Wired LAN Port	<p>It specifies the LAN ports of the AP, including LAN0 and LAN1.</p> <ul style="list-style-type: none"> – LAN0: PoE power supply, data transmission multiplexing port of the AP – LAN1: data transmission port of the AP <p> Tip</p> <p>LAN ports not set as a trunk port can be seen as an access port. You can set a VLAN ID for it.</p>
2.4 GHz SSID	It specifies the currently enabled SSID(s) over the 2.4 GHz/5 GHz band of the AP, and the VLAN IDs corresponding to SSIDs.
5 GHz SSID	
VLAN ID	<p> Tip</p> <p>After the QVLAN function is enabled, the wireless ports corresponding to SSIDs function as access ports. The PVID of an access port is the same as its VLAN ID.</p>

6.8.3 Example of Configuring QVLAN Settings

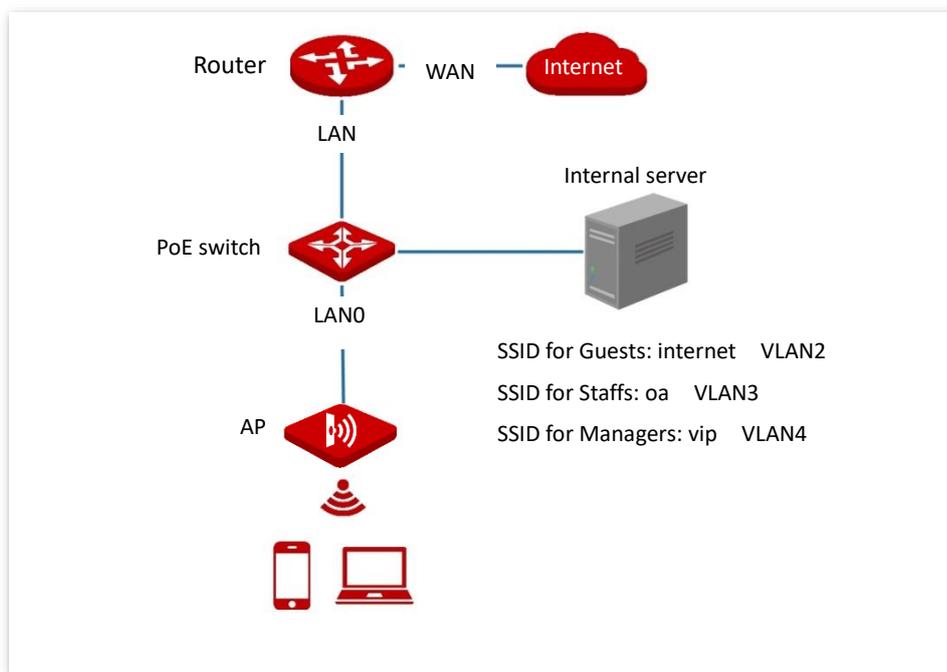
Networking requirement

A hotel has the following wireless network coverage requirements:

- Guests are connected to VLAN 2 and can access only the internet.
- Staffs are connected to VLAN 3 and can access only the LAN.
- Managers are connected to VLAN4 and can access both the LAN and the internet.

Networking assumption

- Set the SSID to **internet** for guests, **oa** for staffs, and **vip** for managers for 2.4 GHz network.
- Configure VLANs for the three SSIDs on AP.
- Configure VLAN forwarding rules on switch.
- Configure VLAN forwarding rules on router and internal server.



Configuration procedure

I. Configure the AP

1. Choose **Wireless > QVLAN Settings**.
2. Enable QVLAN Settings.
3. Modify the VLAN ID of the SSIDs at 2.4 GHz band. Set the VLAN of internet to **2**, oa to **3**, and vip to **4** respectively.
4. Click **Save**.

QVLAN Settings ?

***Enable**

QVLAN Mode

PVID

Management VLAN

Trunk Port LAN0 LAN1

Wired LAN Port VLAN ID (1 to 4094)

LAN0

LAN1

2.4 GHz SSID VLAN ID (1 to 4094)

***internet**

***vip**

***oa**

5 GHz SSID VLAN ID (1 to 4094)

IP-COM_18B03A_5G

5. Click **OK** after confirming the prompted message.

Wait for the automatic reboot of the AP.

II. Configure the switch

Create IEEE 802.1Q VLANs described in the following table on the switch.

Port Connected To	Accessible VLAN ID	Port Type	PVID
AP	1,2,3,4	Trunk	1
LAN server	3,4	Trunk	1
Router	2,4	Trunk	1

Retain the default settings of other ports. For details, refer to the user guide for the switch.

III. Configure the router and internal server

To ensure a normal internet access for wireless clients connected to the AP, the router and internal server must support the QVLAN function and need to be configured. See the following table.

Router:

Port Connected To	Accessible VLAN ID	Port Type	PVID
Switch	2,4	Trunk	1

Internal server:

Port Connected To	Accessible VLAN ID	Port Type	PVID
Switch	3,4	Trunk	1

For details, refer to the user guides for the corresponding devices.

---End

Verification

Wireless clients connected to the **internet** wireless network can only access the internet, wireless clients connected to the **oa** wireless network can only access the LAN. Wireless clients connected to the **vip** wireless network can access both the internet and LAN.

7 Advanced

Traffic Control

The Traffic Control page allows you to set limits on the internet speed of clients to guarantee a proper allocation of limited broadband resources.

By default, the Traffic Control function is disabled. If you want to use this function, configure it on the **Advanced > Traffic Control** page.

Radio Band	SSID	SSID Max. Upload Rate	SSID Max. Download Rate	Client Max. Upload Rate	Client Max. Download Rate	Operation
2.4GHz	IP-COM_81AAE1	No Limit	No Limit	No Limit	No Limit	

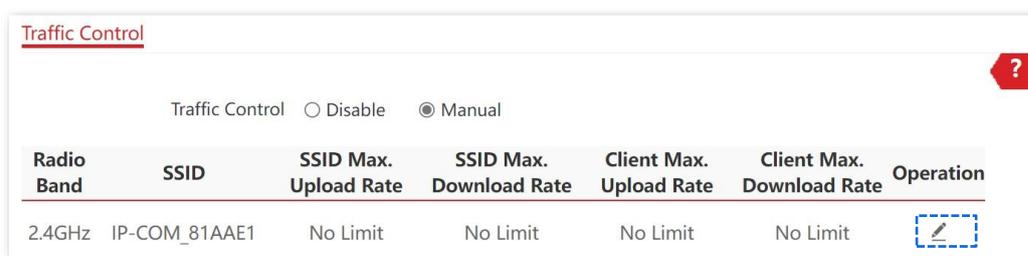
Parameter description

Parameter	Description
Traffic Control	<ul style="list-style-type: none"> - Disable: The Traffic Control function is disabled. - Manual: The Traffic Control function is enabled. The network administrator manually sets SSID and the maximum upload/download rate of user devices to limit the total bandwidth of SSID and evenly allocate bandwidth to users. In this way, if multiple SSIDs are enabled, and a user network with a lower priority (such as guest network) occupies an excessively high internet speed or a user occupies too much bandwidth, such circumstances as excessively low internet speed or even internet unavailability for other users will not occur.
Radio Band	It specifies the radio band of the WiFi network on which you want to set a traffic control rule.
SSID	It specifies the name of the WiFi network on which you want to set a traffic control rule.
SSID Max. Upload Rate	It specifies the maximum upload/download rate allowed for a WiFi network. If you leave it blank, the maximum upload/download rate of the target WiFi network are not limited.
SSID Max. Download Rate	

Parameter	Description
Client Max. Upload Rate	It specifies the maximum upload/download rate allowed for every user device connected to the target WiFi network. If you leave it blank, the maximum upload/download rate of every user device connected to the target WiFi network are not limited.
Client Max. Download Rate	
Operation	Click  to set the maximum upload/download rate allowed for the target WiFi network and the maximum upload/download rate allowed for every user device connected to the target WiFi network.

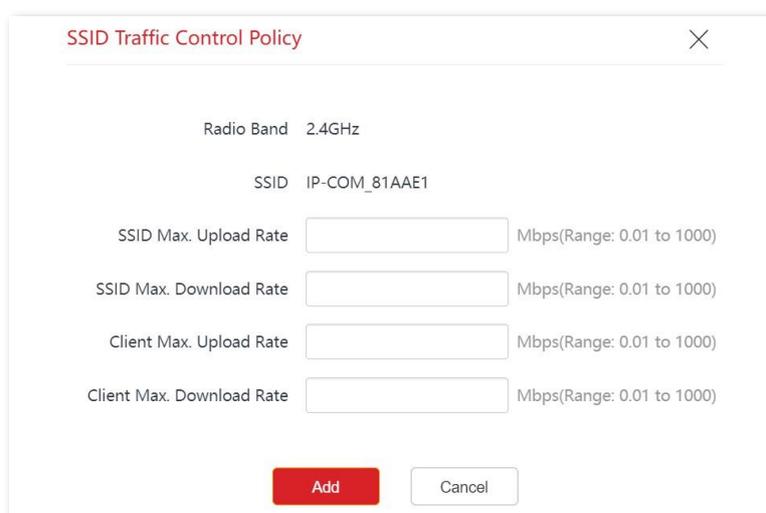
Configure Traffic Control

1. Choose **Advanced > Traffic Control**.
2. Set **Traffic Control** to **Manual**.
3. On the **Traffic Control** list, click  on the row where the WiFi network to be controlled resides.



Radio Band	SSID	SSID Max. Upload Rate	SSID Max. Download Rate	Client Max. Upload Rate	Client Max. Download Rate	Operation
2.4GHz	IP-COM_81AAE1	No Limit	No Limit	No Limit	No Limit	

4. Set the maximum upload/download rate allowed for the WiFi network and the maximum upload/download rate allowed for every user device connected to the WiFi network.
5. Click **Add**.



SSID Traffic Control Policy

Radio Band 2.4GHz

SSID IP-COM_81AAE1

SSID Max. Upload Rate Mbps(Range: 0.01 to 1000)

SSID Max. Download Rate Mbps(Range: 0.01 to 1000)

Client Max. Upload Rate Mbps(Range: 0.01 to 1000)

Client Max. Download Rate Mbps(Range: 0.01 to 1000)

Add

---End

8 Tools

8.1 Date & Time

This section introduces how to set the [system time](#) and [login timeout interval](#) of your AP.

8.1.1 System Time

The **System Time** page allows you to set the system time.

To access the configuration page, choose **Tools > Date & Time > System Time**.

To make the time-related functions effective, ensure that the system time of the AP is set correctly. The AP supports [Sync with Internet Time](#) and [Manual](#) to correct the system time.

Sync with Internet Time

The AP automatically synchronizes its system time with a time server of the internet. This enables the AP to automatically correct its system time after being connected to the internet. For details about how to connect the AP to the internet, refer to [LAN Setup](#).

Parameter description

Parameter	Description
Time Setup	It specifies the mode to set the system time.
Sync Interval	It is valid only when Sync with Internet Time is chosen. It specifies the interval at which the AP will automatically synchronize with a time server of the internet.

Parameter	Description
Time Zone	It is valid only when Sync with Internet Time is chosen. It specifies the standard time zone of the region in which the AP locates.

Manual

You can manually set the system time of the AP. If you choose this option, you need to set the system time each time after the AP reboots.

Enter a correct date and time, or click **Sync with PC Time** to synchronize the system time of the AP with the system time (ensure that it is correct) of the management computer.

8.1.2 Login Timeout Interval

If you log in to the web UI of the AP and perform no operation within the login timeout interval, the AP logs you out for network security. The default login timeout interval is 5 minutes.

The **Login Timeout Interval** page allows you to modify the login timeout interval.

To access the page, choose **Tools > Date & Time > Login Timeout Interval**.

8.2 Maintenance

The Maintenance page allows you to perform the following operations: [reboot](#), [reset](#), [upgrade firmware](#), [back up/restore](#), and [LED indicator control](#).



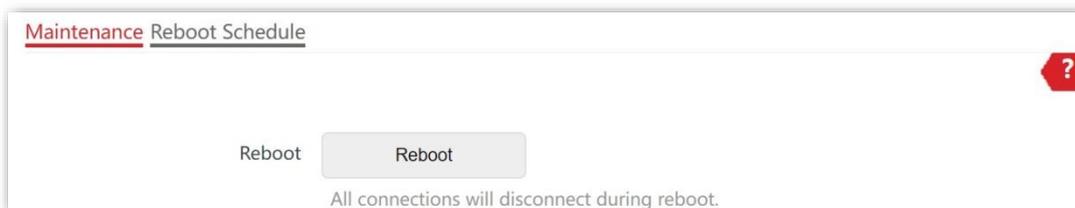
Rebooting the AP disconnects all connections. You are recommended to reboot the AP in spare time.

8.2.1 Reboot

Manual reboot

If a parameter does not take effect or the AP does not work properly, you can try rebooting the AP manually to resolve the problem.

To access the configuration page, choose **Tools > Maintenance > Maintenance**.



Reboot schedule

This function allows the AP to automatically reboot as scheduled. You can use this function to prevent wireless performance degradation or network instability that occurs after a long AP uptime. The AP supports the following two types of scheduled reboot:

- **Reboot Interval:** The AP reboots at the interval you set.
- **Reboot Schedule:** The AP reboots regularly at the time you set.

■ Configure the AP to reboot at an interval



Rebooting at intervals is based on the system time. To avoid reboot time error, ensure that the [system time](#) is correct.

1. Choose **Tools > Maintenance > Maintenance**, and click the **Reboot Schedule** tab.
2. Enable **Reboot Schedule**.
3. Select **Reboot Interval** from the **Type** drop-down list menu.

4. Set **Interval** as required, which is **1440** minutes in this example.
5. Click **Save** to apply your settings.

Maintenance **Reboot Schedule**

Reboot Schedule

Type

Interval min(Range: 10 to 7200)

---End

After the configurations, the AP will automatically reboot in a day.

■ Configure the AP to reboot at specified time

1. Choose **Tools > Maintenance**, and click the **Reboot Schedule** tab.
2. Enable **Reboot Schedule**.
3. Select **Reboot Schedule** from the **Type** drop-down list menu.
4. **Reboot On**: Select the required day(s) when the AP reboots, which is **Monday** in this example.
5. **Reboot At**: Set the time when the AP reboots, which is **3:00** in this example.
6. Click **Save** to apply your settings.

Maintenance **Reboot Schedule**

Reboot Schedule

Type

Reboot On Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday Every Day

Reboot At (Default:3:00)

---End

After the configurations, the AP will automatically reboot at 3:00 every Monday.

8.2.2 Reset

If you cannot locate a fault of the AP or forget the password of the web UI of the AP, you can reset the AP to restore its factory settings and then configure it again.



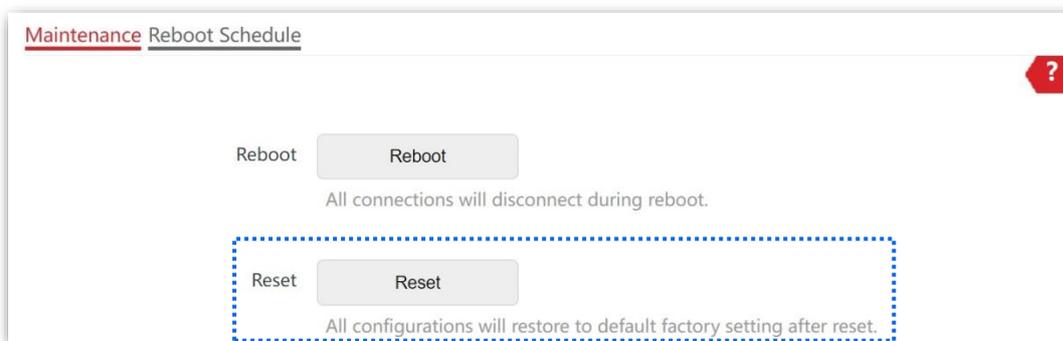
- Resetting the AP deletes all your current configurations, and you need to reconfigure the AP again. Therefore, reset the AP only when necessary.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.
- After the factory settings are restored, the login IP address of the AP is changed to **192.168.0.254**, and the user name and password of the AP are changed to **admin**.

Method 1

After AP completes startup, hold down the reset button for about 10 seconds, and release when the indicator goes out. When the indicator blinks white, the AP is reset.

Method 2

On the **Tools > Maintenance > Maintenance** page, click **Reset**.



8.2.3 Upgrade Firmware

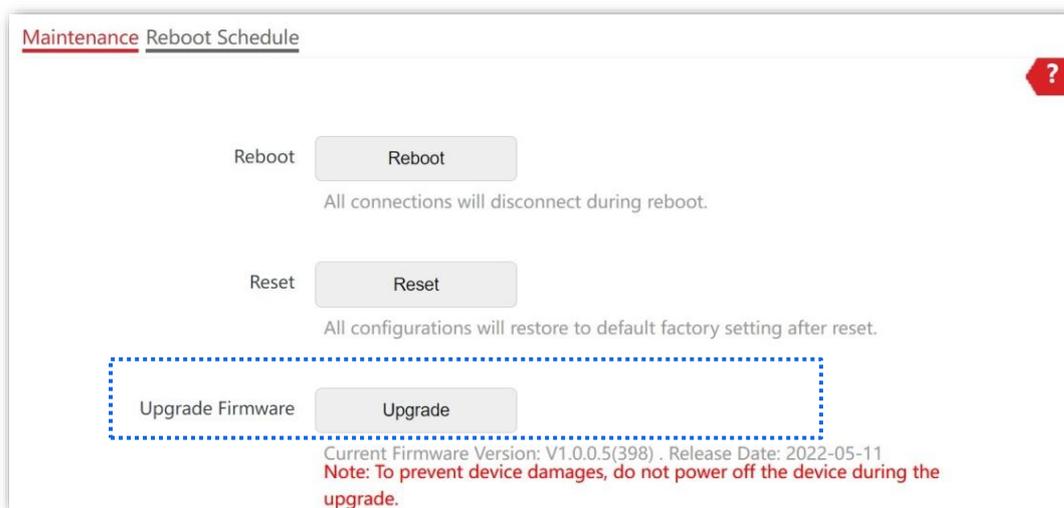
This function enables you to upgrade the AP's firmware to get more functions and higher stability.



- To enable your AP to work properly after an upgrade, ensure that the firmware used to upgrade complies with your product model.
- When upgrading, do not power off the AP.

Procedure

1. Download the latest firmware version for the AP from www.ip-com.com.cn to your local computer, and decompress the package. Generally, the package is in the format of .bin.
2. Log in to the web UI of the AP and choose **Tools > Maintenance > Maintenance**.
3. Click **Upgrade**.



4. Choose the upgrade file in the pop-up window.

---End

Wait until the progress bar completes. Then log in to the web UI of the AP again. Choose **Status > System Status** and check whether the upgrade is successful according to the **Firmware Version** parameter.



If you upgrade low transmit power version to/from high transmit power version, reset the AP after upgrading completes to apply your settings.

8.2.4 Backup/Restore

The backup function is used to export the current configuration of the AP to your computer. The restore function is used to import a configuration file to the AP.

You are recommended to back up the configuration after it is significantly changed. When the performance of your AP decreases because of an improper configuration, or after you restore the AP to factory settings, you can use this function to restore a configuration that has been backed up.

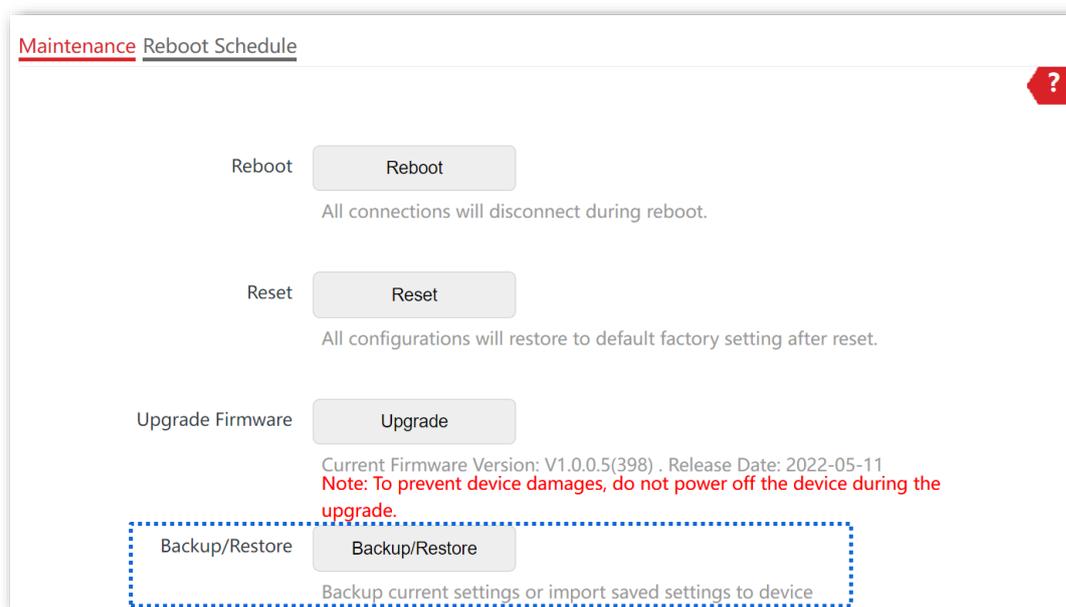


Tip

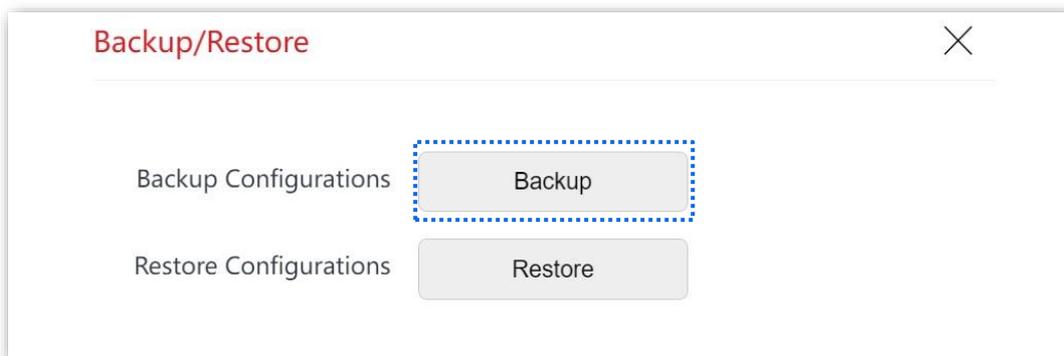
If you need to apply same or similar configuration to many APs, you can configure one of the APs, back up its configuration, and use the backup configuration file to restore the configuration of other APs.

Back up the current configuration

1. Choose **Tools > Maintenance > Maintenance**.
2. Click **Backup/Restore**.



3. Click **Backup** on the pop-up window.



---End

A configuration file indicated with **APCfm.cfg** will be downloaded.

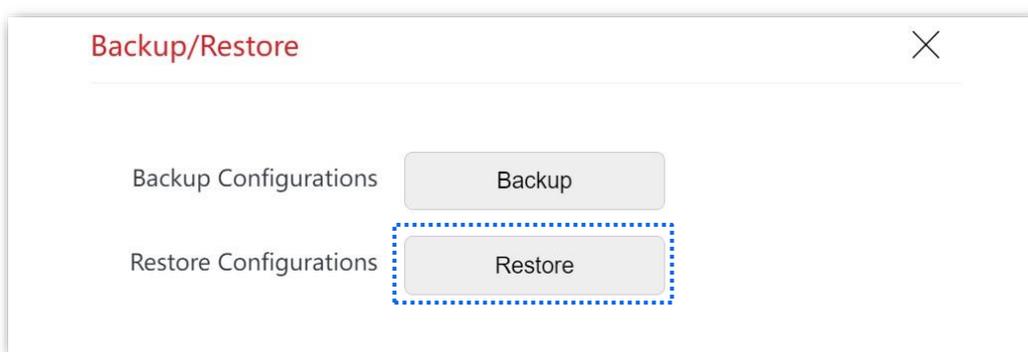


Tip

If the prompt “This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?” appears, click **Keep**.

Restore a configuration

1. Choose **Tools > Maintenance > Maintenance**.
2. Click **Backup/Restore**.
3. Click **Restore** on the pop-up window.



4. Choose the configuration file you backed up.

---End

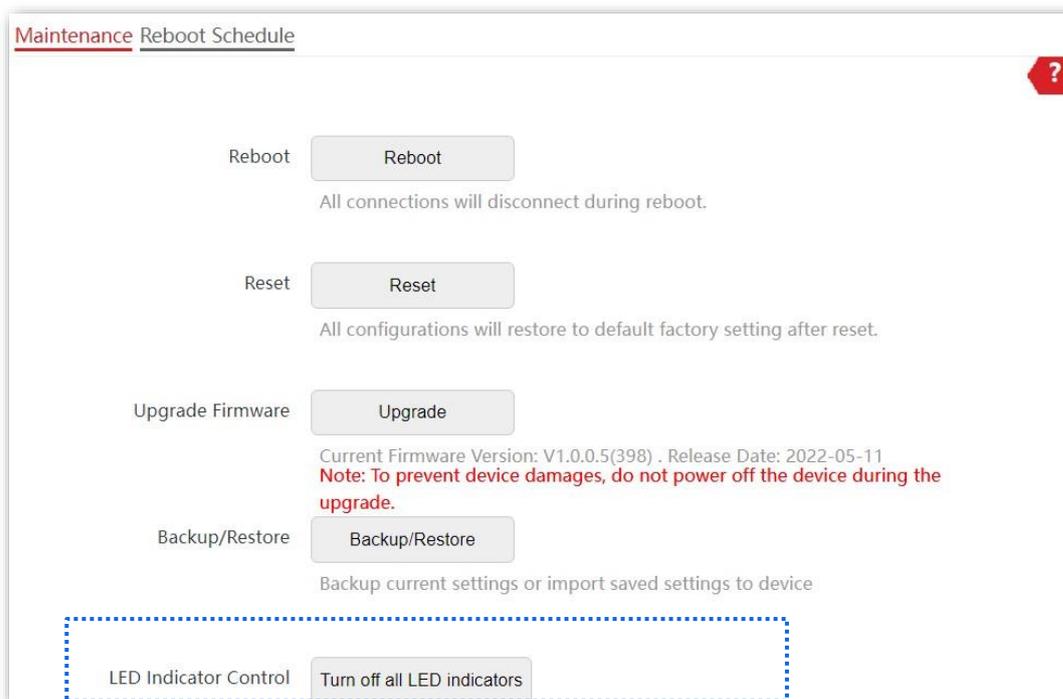
Wait until the progress bar completes.

8.2.5 LED Indicator Control

This function enables you to turn on/off the LED indicator of the AP. By default, the LED indicator is turned on.

Turn off LED indicator

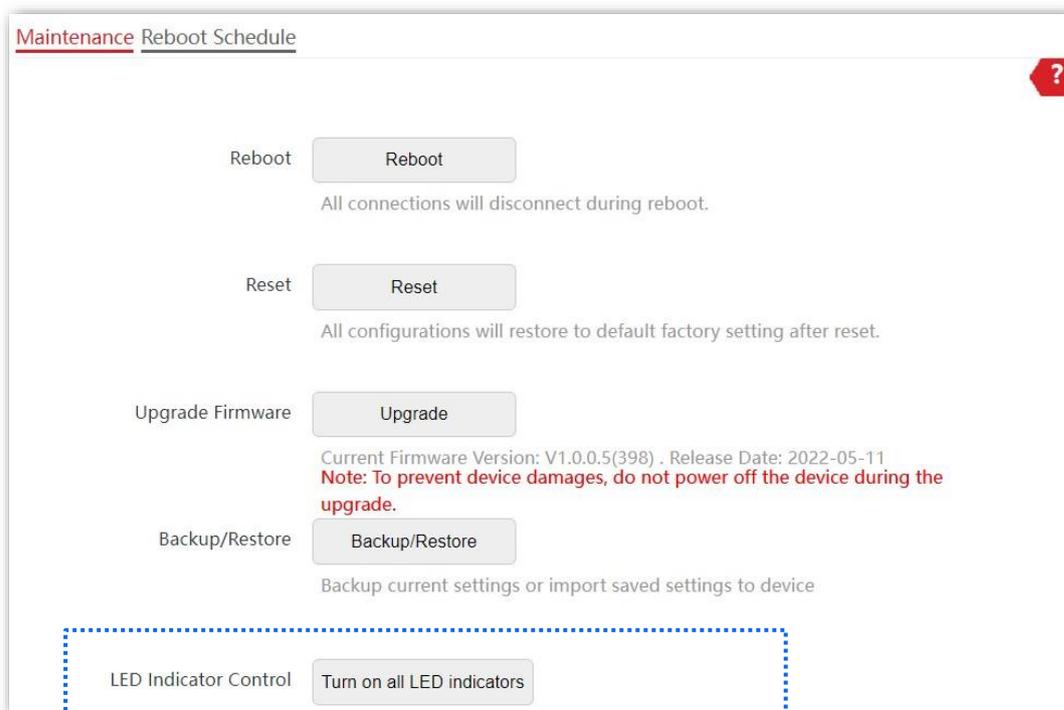
On the **Tools > Maintenance > Maintenance** page, click **Turn off all LED indicators**.



After the configurations, the LED indicator is turned off and no longer displays the working status of the AP.

Turn on LED indicator

On the **Tools > Maintenance > Maintenance** page, click **Turn on all LED indicators**.



After the configurations, the LED indicator lights up again and you can judge the working status of the AP.

8.3 Account

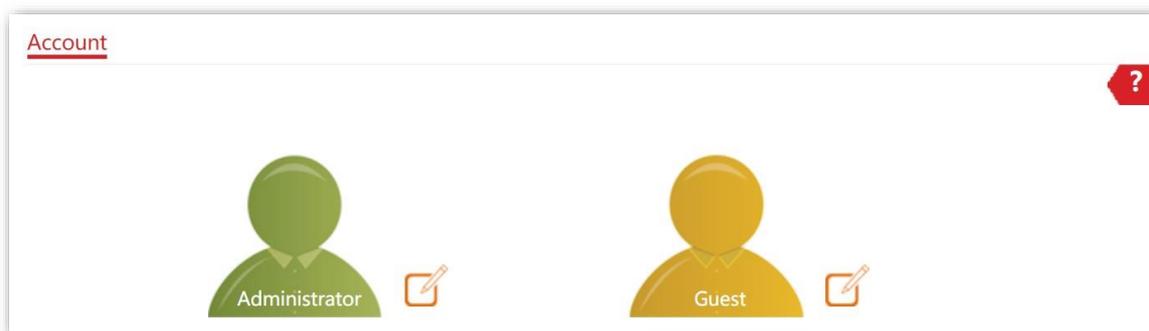
8.3.1 Overview

The **Account** page allows you to modify the information of the login account to keep unauthorized users from entering the web UI and modifying configurations, thus protecting the wireless network.

To access the page, choose **Tools > Account**.

The AP supports two account types: **Administrator** and **Guest**.

- **Administrator**: This account type has permission to view and modify the settings. The default username and password for this account are **admin/admin** (both are case-sensitive).
- **Guest**: This account type can only view other than modifying the settings. The default username and password for this account are **user/user** (both are case-sensitive). This account type is disabled by default.



8.3.2 Modify the password and user name of login account

1. Choose **Tools > Account**.
2. Click  beside the account to be modified.
3. If the account to be modified is a Guest, enable the **Guest Account** first. Otherwise, go to the next step.
4. Enter the current password in **Old Password**.
5. Enter the new account name, for example, **123**, in **New User Name**.
6. Enter the new password in **New Password** and **Confirm Password**.
7. Click **Save**.

Administrator Account ✕

Old User Name

Old Password

New User Name

New Password

Confirm Password

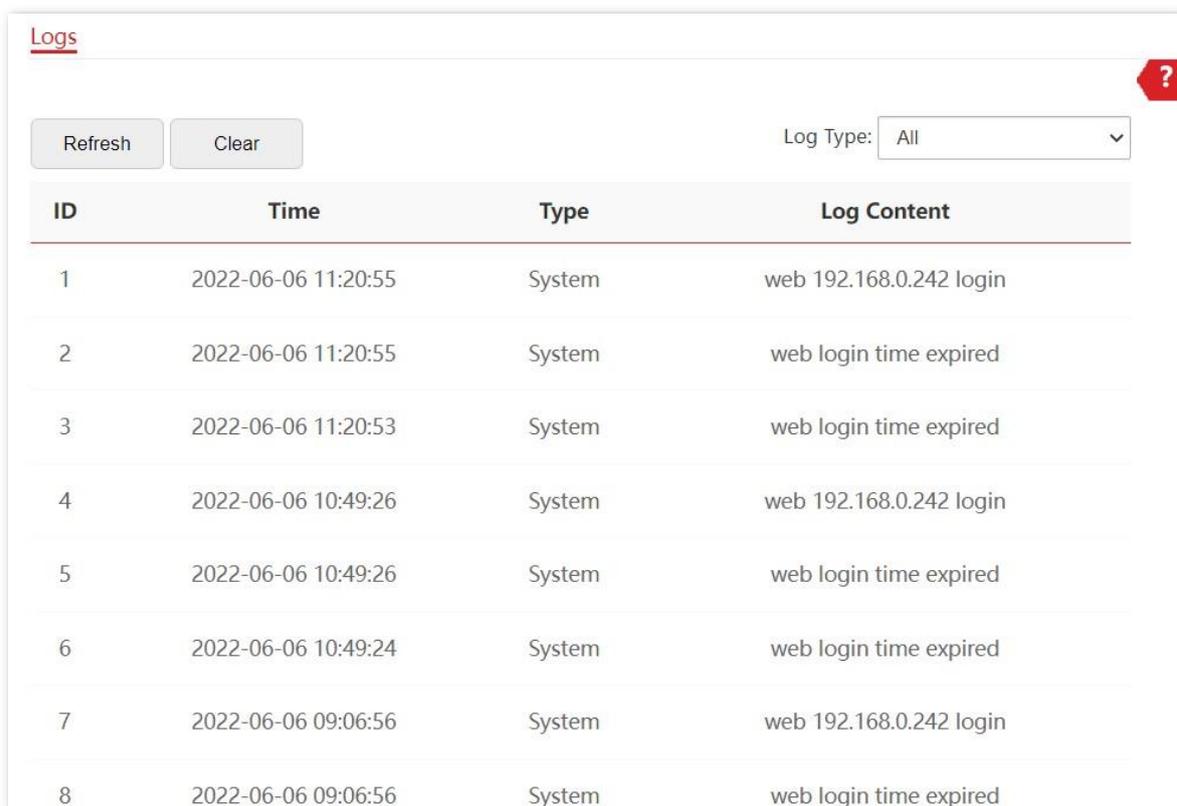
---End

8.4 System Log

The Logs page allows you to view system logs.

The logs of the AP record various events that occur and the operations that users perform after the AP starts. In case of a system fault, you can refer to the logs during troubleshooting.

To access the page, choose **Tools > System Log > Logs**.



ID	Time	Type	Log Content
1	2022-06-06 11:20:55	System	web 192.168.0.242 login
2	2022-06-06 11:20:55	System	web login time expired
3	2022-06-06 11:20:53	System	web login time expired
4	2022-06-06 10:49:26	System	web 192.168.0.242 login
5	2022-06-06 10:49:26	System	web login time expired
6	2022-06-06 10:49:24	System	web login time expired
7	2022-06-06 09:06:56	System	web 192.168.0.242 login
8	2022-06-06 09:06:56	System	web login time expired

To ensure that the logs are recorded correctly, verify the system time of the AP. You can [correct the system time of the AP](#) by choosing **Tools > Time & Date > System Time**.



When the AP reboots, the previous logs are lost.

The AP reboots when the AP is powered on after a power failure, the QVLAN function is configured, the firmware is upgraded, an AP configuration is backed up or restored, or the factory settings are restored.

8.5 Diagnostic Tool

With the diagnostics tool, you can detect the connection status and connection quality of a network.

Procedure

The link to **www.google.com** is used as an example.

1. Choose **Tools > Diagnostics Tool**.
2. Enter the IP address or domain name to be pinged in **Target IP /Domain Name**. In this example, enter **www.google.com**.
3. Click **ping**.



---End

The diagnosis result will be displayed in a few seconds in the black text box below. See the following figure.



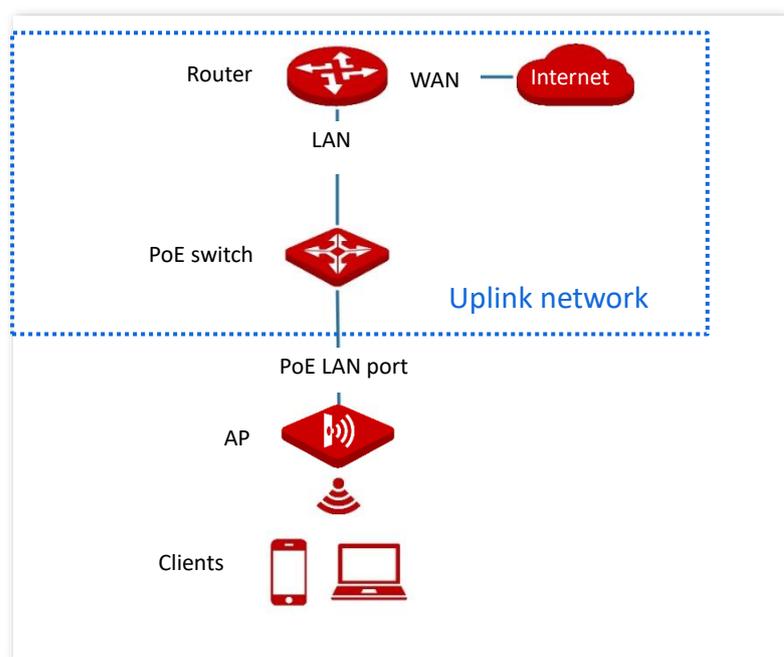
8.6 Uplink Detection

8.6.1 Overview

In AP mode, the AP connects to its upstream network using the PoE LAN port. If a critical node between the PoE LAN port and the upstream network fails, the AP as well as the wireless clients connected to the AP cannot access the upstream network. If uplink check is enabled, the AP regularly pings specified hosts through the PoE LAN port. If all the hosts are not reachable, the AP stops its wireless service and wireless clients cannot find the SSIDs of the AP. The client can reconnect to the AP only after the connection between the AP and the upstream networks is recovered.

If the uplink of the AP with uplink check enabled is faulty, wireless clients can connect to the upstream network through another nearby AP that works properly.

See the following topology (The PoE LAN port serves as the uplink port).



8.6.2 Configure Uplink Detection

1. Choose **Tools > Uplink Check**.
2. Enable **Uplink Detection**.
3. Enter the IP address of the host to be pinged in **Host1 to Ping** or **Host2 to Ping**, such as the IP address of the switch or router directly connected to the Ethernet port of the AP. If there is only one host IP address, enter this IP address in both **Host1 to Ping** and **Host2 to Ping**.
4. Set **Ping Interval** to the interval at which the AP detects its uplink. The default value is **10** minutes.
5. Click **Save**.

Uplink Detection

Uplink Detection

Host1 to Ping

Host2 to Ping

Ping Interval min(Range: 10 to 100. Default: 10)

Save

---End

Appendixes

Factory default settings

The following table lists the default values of major parameters of the AP.

Parameter		Default Value
	Management IP address	192.168.0.254
Login	User Name/Password	Administrator admin admin
		Guest user user
Quick Setup	Working Mode	AP Mode
LAN Setup	IP Address Type	Static IP Address
	IP Address	192.168.0.254
	Subnet Mask	255.255.255.0
SSID Settings	SSID	2.4 GHz The AP allows 8 SSIDs. By default, the primary SSID is enabled, and the other SSIDs are disabled.
		5 GHz The AP allows 8 SSIDs. By default, the primary SSID is enabled, and the other SSIDs are disabled.
RF Settings	Wireless Network	Enable

Acronyms & Abbreviations

Acronyms & Abbreviations	Full Name
AC	Access Point Controller
AES	Advanced Encryption Standard
AIFSN	Arbitration Inter Frame Spacing Number
AP	Access Point
APSD	Automatic Power Save Delivery
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EDCA	Enhanced Distributed Channel Access
LAN	Local Area Network
MIB	Management Information Base
MU-MIMO	Multi-User Multiple-Input Multiple-Output
OFDMA	Orthogonal Frequency Division Multiple Access
PoE	Power over Ethernet
PSK	Pre-shared Key
PVID	Port-base VLAN ID
SAE	Simultaneous Authentication of Equals
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
TXOP	Transmission Opportunity
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WMM	Wi-Fi multi-media
WPA	Wi-Fi Protected Access