

# User Guide

## Ceiling AP Series

## Copyright Statement

©2019 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! Please read this user guide before you start.

## Conventions

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

Item	Presentation	Example
Cascading menus	>	Internet Settings > LAN Setup
Parameter and value	Bold	Set <b>SSID</b> to <b>Tom</b> .
Variable	Italic	Format: <i>XX:XX:XX:XX:XX:XX</i>
UI control	Bold	On the <b>Quick Setup</b> page, click the <b>Save</b> button.

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 device.
 Tip	This format is used to highlight a procedure that will save time or resources.

## Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
AC	Access Controller (Network Equipment)
AC	Access Category (WMM settings)
ACK	Acknowledge
AES	Advanced Encryption Standard
AIFSN	Arbitration Inter Frame Spacing Number
AP	Access Point
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
BE	Best Effort
BK	Background
CAT5e	Category 5 Ethernet
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance

Acronym or Abbreviation	Full Spelling
CTS	Clear To Send
Cwmax	Contention Window Maximum
Cwmin	Contention Window Minimum
DHCP	Dynamic Host Configuration Protocol
DIFS	Distributed Inter-Frame Spacing
DNS	Domain Name Server
DTIM	Delivery Traffic Indication Message
EDCA	Enhanced Distributed Channel Access
GI	Guard Interval
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Medium Access Control
MIB	Management Information Base
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NMS	Network Management System
NTS	Network Time Server
OID	Object Identifier
PoE	Power-over-Ethernet
PPP	Point to Point Protocol
PVID	Port-based VLAN ID
QVLAN	802.11q VLAN
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RTS	Request To Send
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
STA	Station
SYS	System
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TXOP	Transmission Opportunity
UI	User Interface
UTF-8	8-bit Unicode Transformation Format
VI	Video Stream
VID	Virtual ID
VLAN	Virtual Local Area Network
VO	Voice Stream
WAN	Wide Area Network

Acronym or Abbreviation	Full Spelling
WEP	Wired Equivalent Privacy
WMF	Wireless Multicast Forwarding
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPA-PSK	Wi-Fi Protected Access-Pre-shared Key

## 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](mailto:info@ip-com.com.cn)



<http://www.ip-com.com.cn>

# Contents

<b>1 Login.....</b>	<b>1</b>
1.1 Logging in to the web UI of the AP .....	1
1.2 Logging out.....	2
1.3 Web UI layout .....	3
1.4 Frequently-used buttons .....	4
<b>2 Status.....</b>	<b>5</b>
2.1 System status .....	5
2.2 Wireless status.....	7
2.3 Traffic statistics .....	9
2.4 Client list.....	10
<b>3 Working mode.....</b>	<b>12</b>
3.1 AP mode (default mode) .....	12
3.1.1 Typical network topology .....	12
3.1.2 Getting familiar with AP mode configuration page .....	13
3.1.3 Configuring AP mode .....	13
3.2 Client+AP mode.....	15
3.2.1 Typical network topology .....	15
3.2.2 Getting familiar with Client+AP mode configuration page .....	15
3.2.3 Configuring Client+AP mode.....	16
<b>4 Internet settings.....</b>	<b>18</b>

4.1 LAN setup.....	18
4.1.1 Overview .....	18
4.1.2 Configuring the AP to obtain IP address automatically (for multiple APs) .....	20
4.1.3 Configuring the AP to use static IP address (for few APs) .....	21
4.2 DHCP server .....	22
4.2.1 Overview .....	22
4.2.2 Configuring DHCP server of the AP .....	23
4.2.3 Viewing DHCP clients.....	24
<b>5 Wireless .....</b>	<b>25</b>
5.1 SSID .....	25
5.1.1 Overview .....	25
5.1.2 Modifying SSID-related parameters .....	28
5.1.3 Example of configuring a WiFi network encrypted by WPA or WPA2 .....	30
5.2 RF settings.....	49
5.2.1 Overview .....	49
5.2.2 Configuring RF settings.....	51
5.3 RF optimization .....	52
5.3.1 Overview .....	52
5.3.2 Modifying radio optimization settings .....	54
5.4 Frequency analysis .....	56
5.4.1 Viewing frequency analysis .....	56
5.4.2 Executing channel scan.....	56
5.5 WMM .....	58
5.5.1 Overview .....	58
5.5.2 Configuring scenario-based WMM settings.....	60
5.5.3 Configuring WMM settings manually .....	61
5.6 Access control.....	62
5.6.1 Overview .....	62

5.6.2 Configuring access control.....	63
5.7 Advanced settings.....	65
5.7.1 Identify client type .....	65
5.7.2 Broadcast packet filter .....	66
5.8 QVLAN settings.....	67
5.8.1 Overview.....	67
5.8.2 Example of configuring QVLAN .....	68
<b>6 Advanced .....</b>	<b>72</b>
6.1 Deployment mode .....	72
6.1.1 Applicable scenarios.....	72
6.1.2 Introduction to deployment mode of the AP.....	74
6.1.3 Configuring the cloud deployment mode.....	75
6.2 SNMP .....	77
6.2.1 Overview.....	77
6.2.2 Configuring the SNMP function.....	79
6.2.3 Example of configuring SNMP settings.....	80
<b>7 Tools.....</b>	<b>82</b>
7.1 Date & time .....	82
7.1.1 Overview.....	82
7.1.2 Configuring system time.....	83
7.1.3 Configuring login timeout interval.....	84
7.2 Maintenance.....	86
7.2.1 Reboot .....	86
7.2.2 Reset.....	88
7.2.3 Upgrade firmware .....	89
7.2.4 Backup and restoring configurations .....	91
7.2.5 LED indicator control.....	92
7.3 Account.....	93



7.3.1 Overview .....	93
7.3.2 Modifying login password.....	93
7.4 System Log .....	94
7.4.1 Viewing system logs .....	94
7.4.2 Modifying number of logs to be displayed on Web UI .....	95
7.4.3 Sync system logs of the AP to a log server .....	95
7.5 Diagnostic tool .....	98
7.5.1 Overview .....	98
7.5.2 Executing Ping command to detect connection quality.....	98
7.6 Uplink check.....	100
7.6.1 Overview .....	100
7.6.2 Configuring uplink detection .....	100
<b>Appendix .....</b>	<b>102</b>

# 1 Login

## 1.1 Logging in to the web UI of the AP

Before you start, ensure that:

- The AP is properly connected to a computer with an Ethernet cable.
- The IP address of the management computer is in the same network segment of the AP. For example, if the IP address of the AP is 192.168.0.254, the management computer should be configured with an IP address of 192.168.0.X (X: 2~253). For how to configure the computer with a specified IP address, see [A.1](#) in Appendix.

### Procedure

1. Start a web browser on the computer, enter the IP address of the AP (default: **192.168.0.254**) in the address bar, and press **Enter** (Windows) or **Return** (Mac) on the keyboard.

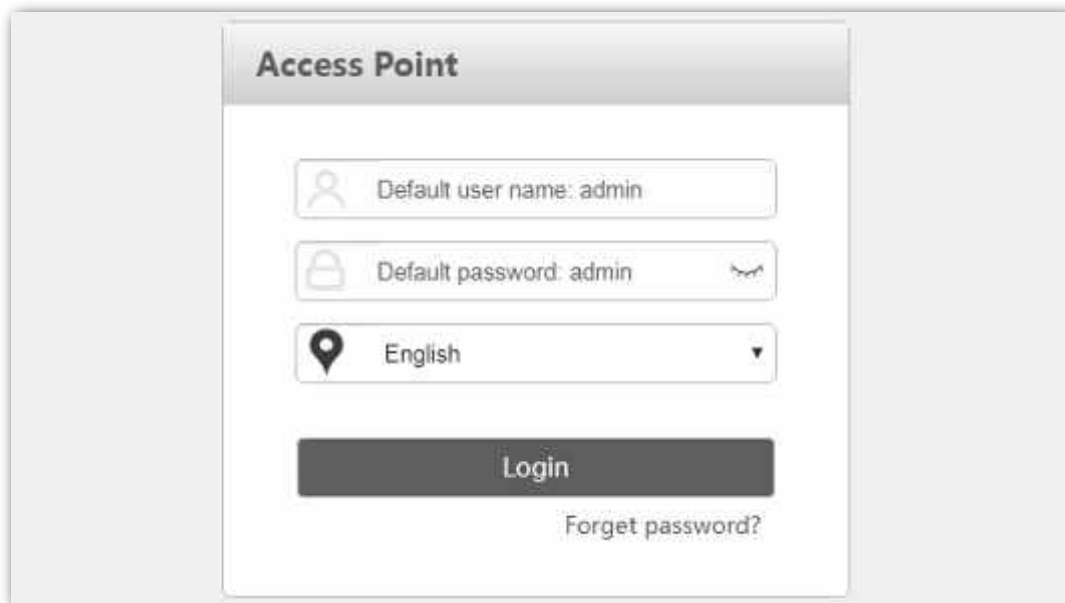


Note

How to obtain the login IP address:

- The default login IP address is **192.168.0.254**, which could be found on the rear panel of the AP. You are recommended to note it down and keep it safely for later use.
- If the AP is managed by an IP-COM AC (access controller) or an IP-COM router with AP functionality, the IP address of the AP is assigned by the management IP-COM AC or router. To obtain it, go to the web UI of the AC or the router to view the new IP address of the AP.

2. Enter the user name and password (default: **admin/admin**), and click **Login**.

The image shows a web-based login interface for an Access Point. It features a central white box with a grey header labeled "Access Point". Inside the box, there are three input fields: the first is for the "Default user name: admin" with a person icon; the second is for the "Default password: admin" with a lock icon and a toggle for visibility; the third is a language dropdown menu currently set to "English" with a location pin icon. Below these fields is a large grey "Login" button. At the bottom right of the box is a link that says "Forget password?".

Note

- If the login page does not appear, refer to [Q1 in A.2 FAQ](#).
- To modify the login user name and password, see Account.

---End

## 1.2 Logging out

The system logs you out when you:

- Close the web browser.
- Log in to the web UI of the AP but perform no operation within the **Login Timeout Interval** (default: 5 minutes).



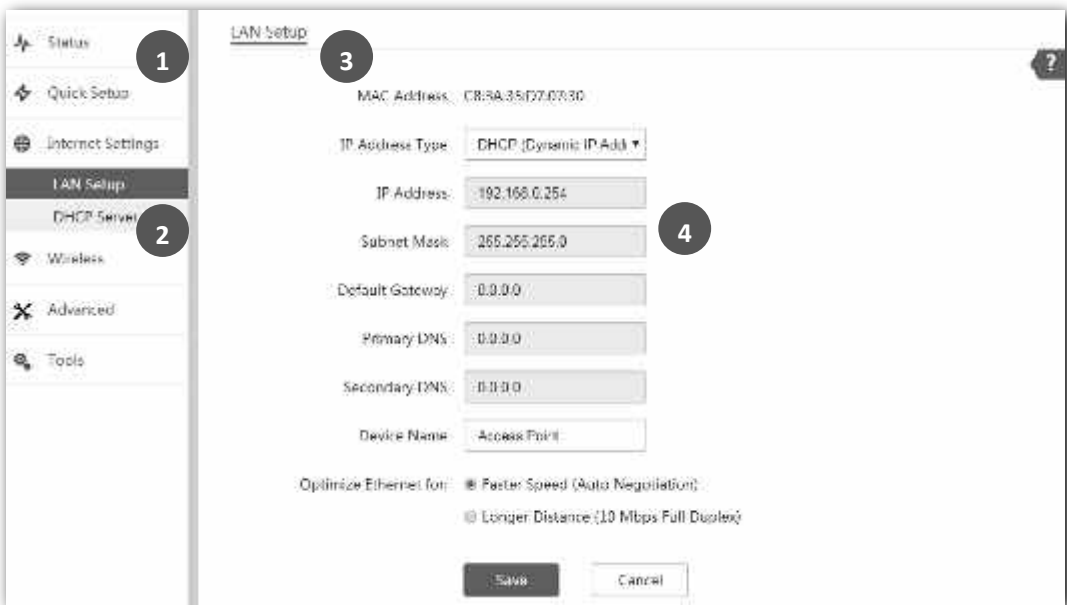
Tip

**Login Time Interval** allows you to set how long you can stay on the web UI, which could be modified by navigating to **Tools > Date & Time > Login Timeout Interval**.

---

## 1.3 Web UI layout

The web UI of the AP consists of four sections, including the level-1, and level-2 navigation bars, tab page area, and the configuration area. See the following figure.






No.	Name	Description
1	Level-1 navigation bar	Used to display the function menu of the AP. Users can select functions in the navigation bars and the configuration appears in the configuration area.
2	Level-2 navigation bar	
3	Tab page area	
4	Configuration area	Used to modify or view your configuration.



The functions and parameters dimmed on the web UI indicate that they cannot be changed in the current configuration or they are not supported by the AP. To configure such functions or parameters, configure their related functions or parameters first.

## 1.4 Frequently-used buttons

The following table describes the frequently-used buttons available on the web UI of the AP.

Button	Description
	Used to save the configuration on the current page and enable the configuration to take effect.
	Used to modify the current configuration on the current page back to the original configuration.
	Used to get the online help.

## 2 Status

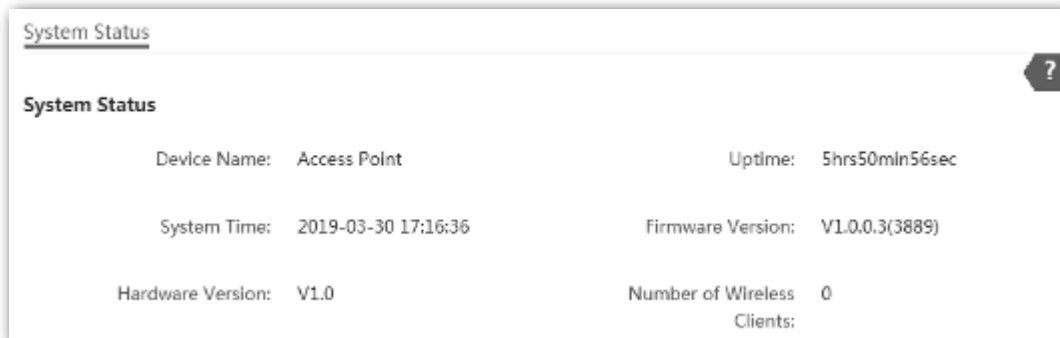
This module presents you with an overall running status of the AP, including system status, LAN port status, wireless status (2.4 GHz and 5 GHz), traffic statistics, and information of wireless clients connected to the AP. You are allowed to view rather than modifying here.

### 2.1 System status

This page displays the [System Status](#) and [LAN Port Status](#) of the AP.

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

- **System Status**



#### Parameter description

Parameter	Description
Device Name	It specifies the name of the AP. You can modify it on <b>Internet Settings &gt; LAN Setup</b> page.
Uptime	It specifies the time that has elapsed since the AP starts up last time.

It specifies the current system time of the AP.

System Time



To make time-related configurations work properly, ensure that the system time is correct. You can modify it on **Tools > Date & Time** page.

Firmware Version

It specifies the current firmware version number of the AP.

Hardware Version

It specifies the current hardware version number of the AP.

Number of Wireless Client

It specifies the quantity of wireless devices currently connected to the AP.

#### ■ LAN Port Status



#### Parameter description

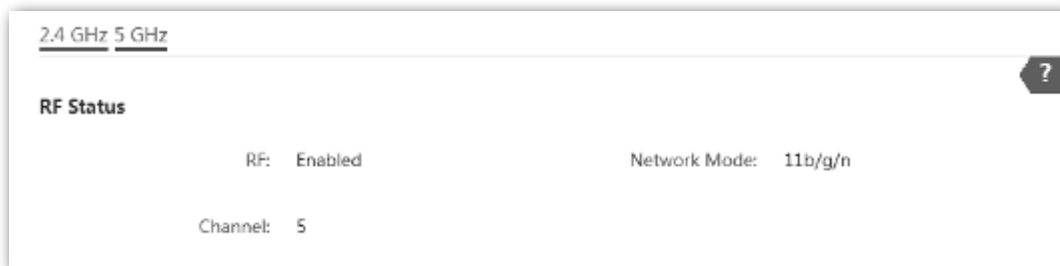
Parameter	Description
MAC Address	<p>It specifies the physical address of the AP's LAN port.</p> <p>If you connect the AP to other devices using Ethernet cables, the AP uses this MAC address to communicate with those devices.</p>
IP Address	<p>It specifies the IP address of the AP's LAN port, which can be used to log in to the web UI.</p> <p>You can modify it on <b>Internet Settings &gt; LAN Setup</b> page.</p>
Subnet Mask	<p>It specifies the subnet mask of the AP.</p>
Primary DNS Server	<p>It specifies the primary DNS server of the AP.</p>
Secondary DNS Server	<p>It specifies the secondary DNS server of the AP.</p>

## 2.2 Wireless status

This page displays radio information and SSID information of the AP. You can get a glance of whether or not the radio frequency (RF) function is enabled, the network mode it currently uses, and the channel it operates, as well as all the SSIDs-related information. This page includes [RF status](#) and [SSID status](#).

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

### ■ RF status



### Parameter description


Parameter	Description
RF	It specifies whether the WiFi network at the corresponding band is enabled. <ul style="list-style-type: none"><li>- <b>Enabled:</b> WiFi network at the corresponding band is enabled.</li><li>- <b>Disabled:</b> WiFi network at the corresponding band is disabled.</li></ul>
Network Mode	It specifies the network mode currently enabled by the AP on each radio band.
Channel	It specifies the current channel the AP operates on either 2.4 GHz or 5 GHz band.



## ■ SSID status

SSID Status			
SSID	MAC Address	Status	Security Mode
W63APV1.0-TEST	C8:3A:35:D7:07:31	Enabled	None
IP-COM_D70731	C8:3A:35:D7:07:32	Disabled	None
IP-COM_D70732	C8:3A:35:D7:07:33	Disabled	None
IP-COM_D70733	C8:3A:35:D7:07:34	Disabled	None
IP-COM_D70734	C8:3A:35:D7:07:35	Disabled	None
IP-COM_D70735	C8:3A:35:D7:07:36	Disabled	None
IP-COM_D70736	C8:3A:35:D7:07:37	Disabled	None
IP-COM_D70737	C8:3A:35:D7:07:38	Disabled	None

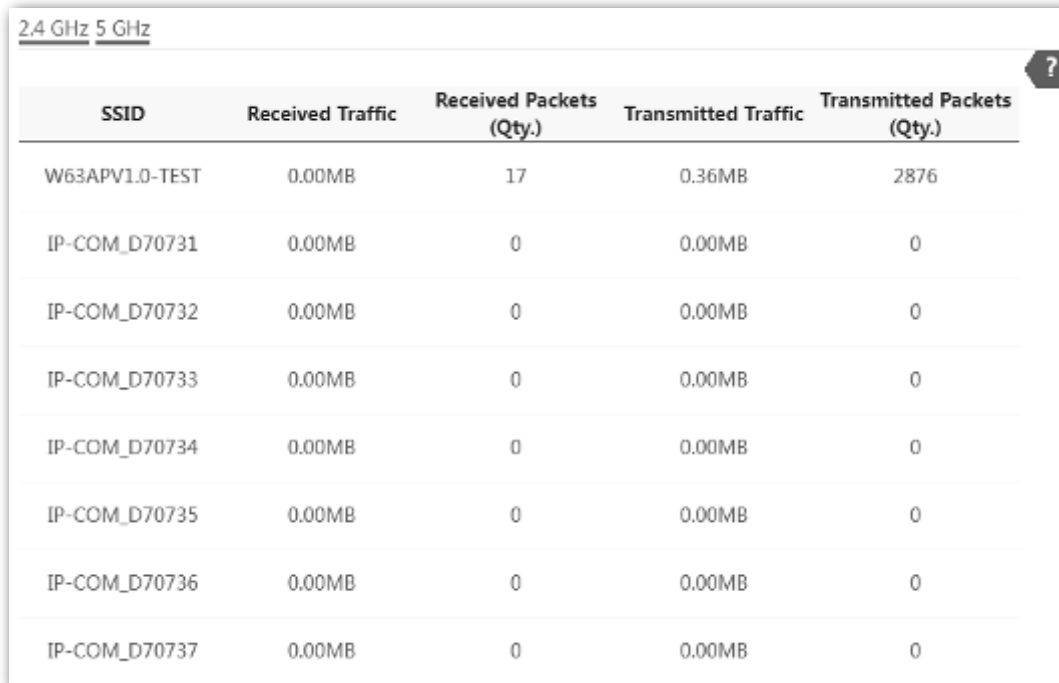
## Parameter description

Parameter	Description
	Wireless network name of the AP. The AP supports up to <b>8 SSIDs</b> on <b>2.4 GHz</b> and <b>4 SSIDs</b> on <b>5 GHz</b> .
SSID	 Tip The 1st SSID on the list indicates the <b>primary</b> SSID. By default, only the primary SSID on each radio band is enabled.
MAC Address	It specifies the physical address of the corresponding wireless network.
Status	It specifies whether or not the corresponding WiFi network is enabled.
Security Mode	It specifies the security mode adopted by the corresponding WiFi network.

## 2.3 Traffic statistics

This page allows you to view statistical information about traffic based on SSIDs.

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

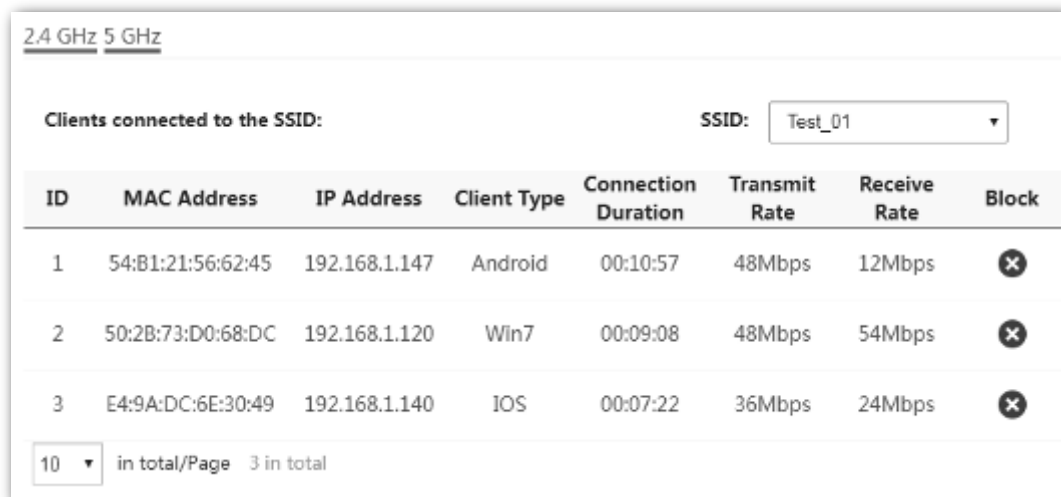


SSID	Received Traffic	Received Packets (Qty.)	Transmitted Traffic	Transmitted Packets (Qty.)
W63APV1.0-TEST	0.00MB	17	0.36MB	2876
IP-COM_D70731	0.00MB	0	0.00MB	0
IP-COM_D70732	0.00MB	0	0.00MB	0
IP-COM_D70733	0.00MB	0	0.00MB	0
IP-COM_D70734	0.00MB	0	0.00MB	0
IP-COM_D70735	0.00MB	0	0.00MB	0
IP-COM_D70736	0.00MB	0	0.00MB	0
IP-COM_D70737	0.00MB	0	0.00MB	0




## 2.4 Client list

This page allows you to view wireless clients connected to each SSID of the AP and their basic information, and to block unknown wireless clients. Here, “client” refers to the devices connected to the AP’s wireless networks.

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





The screenshot shows the 'Client List' interface. At the top, there are tabs for '2.4 GHz' and '5 GHz'. Below them, it says 'Clients connected to the SSID:' followed by a dropdown menu for 'SSID:' with 'Test\_01' selected. The main part of the interface is a table with the following columns: ID, MAC Address, IP Address, Client Type, Connection Duration, Transmit Rate, Receive Rate, and Block. There are three rows of data. At the bottom, there is a pagination bar showing '10' in a dropdown, 'in total/Page', and '3 in total'.

ID	MAC Address	IP Address	Client Type	Connection Duration	Transmit Rate	Receive Rate	Block
1	54:B1:21:56:62:45	192.168.1.147	Android	00:10:57	48Mbps	12Mbps	
2	50:2B:73:D0:68:DC	192.168.1.120	Win7	00:09:08	48Mbps	54Mbps	
3	E4:9A:DC:6E:30:49	192.168.1.140	IOS	00:07:22	36Mbps	24Mbps	

10 in total/Page 3 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 physical address of the client.
IP Address	It specifies the IP address of the client.
Client Type	<div>It specifies the operating system of the client.</div> <div> Tip</div> <div>The AP identifies the client type on two conditions:<ul style="list-style-type: none"><li>– The <b>Identity Client Type</b> function is enabled (To enable it, navigate to <b>Wireless &gt; Advanced Settings</b>).</li><li>– The client connected to the AP has accessed an <b>http://</b> website.</li></ul>Otherwise, -- is displayed.</div>
Connection Duration	It specifies the online time of the client.
Transmit Rate	It specifies the real time traffic the client has transmitted.
Receive Rate	It specifies the real time traffic the client has received.
Block	Click  to block the client from accessing the AP’s wireless network.

Parameter	Description
	To unblock a client, navigate to <b>Wireless &gt; Access Control</b> .

---

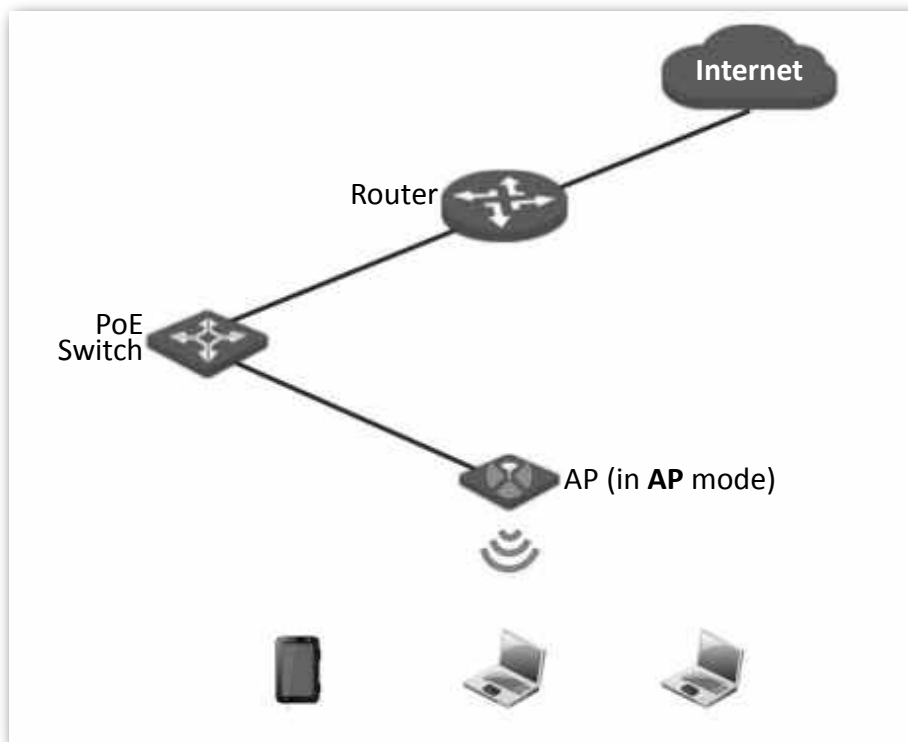
# 3 Working mode

The AP supports **AP** mode (default mode) and **Client+AP** mode. This chapter introduces how to set the working mode of the AP.

## 3.1 AP mode (default mode)

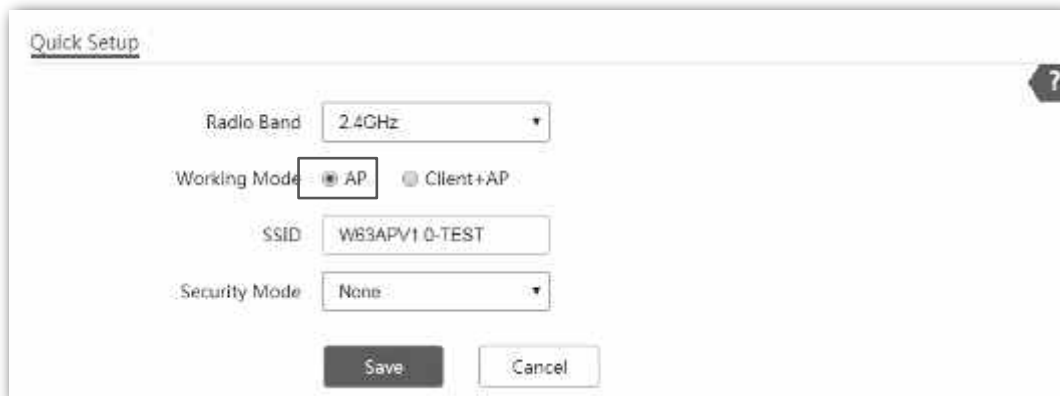
### 3.1.1 Typical network topology

In this mode, the AP connects to the internet in a wired manner, and converts wired network into wireless network. See the following typical network topology.




### 3.1.2 Getting familiar with AP mode configuration page

To access the configuration page, choose **Quick Setup**.



#### Parameter description

Parameter	Description
Radio Band	It is used to select the radio band for configurations.
Working Mode	<p>It specifies the working modes supported by the device.</p> <ul style="list-style-type: none"><li>- <b>AP</b> mode (default mode): This mode is used to deploy wireless networks by connecting the AP to the internet in a wired manner.</li><li>- <b>Client+AP</b> mode: This mode is used to extend the existing wireless network by bridging the upstream wireless signals.</li></ul>
SSID	<p>Primary Wireless network name of the AP.</p> <p> <b>Tip</b></p> <p>The 1st SSID on each radio band indicates the <b>primary</b> SSID.</p>
Security Mode	<p>It specifies the security mode you set for your AP's WiFi network, including <b>None</b>, <b>WEP</b>, <b>WPA-PSK</b>, <b>WPA2-PSK</b>, <b>Mixed WPA/WPA2-PSK</b>, <b>WPA</b> and <b>WPA2</b>.</p> <p>See <a href="#">Security Mode</a> for details.</p>

### 3.1.3 Configuring AP mode

Log in to the web UI of the AP, and choose **Quick Setup** to enter the configuration page first.



- By default, the device works in **AP** mode.
- The following introduces how to set the device into AP mode on 2.4 GHz band. Configuration on 5 GHz is identical.
- The device supports up to **8 SSIDs** on **2.4 GHz** band and **4 SSIDs** on **5 GHz** band. The SSID-related parameters on this page refer to the first (primary) SSID of the AP.

### Before you start:

Ensure that the upstream router has connected to the internet successfully.

### Procedure

1. Select **2.4 GHz** from the **Radio Band** drop-down list menu.
2. Set **Working Mode** to **AP**.
3. Customize an SSID (wireless network name) in the **SSID** box, which is **IP-COM\_WiFi** in this example.

This SSID is also your primary SSID on 2.4 GHz band.

4. Select the security mode from the **Security Mode** drop-down list menu, which is **WPA2-PSK** in this example.
5. Select the **Encryption Algorithm**, which is **AES** in this example.
6. Set a WiFi password in the **Key** box.
7. Click **Save** to apply your settings.

The screenshot shows a 'Quick Setup' window with the following fields and options:

- Radio Band:** A dropdown menu set to '2.4 GHz'.
- Working Mode:** Two radio buttons, 'AP' (selected) and 'Client+AP'.
- SSID:** A text box containing 'IP-COM\_WiFi'.
- Security Mode:** A dropdown menu set to 'WPA2-PSK'.
- Encryption Algorithm:** Three radio buttons, 'AES' (selected), 'TKIP', and 'TKIP&AES'.
- Key:** A text box with a masked password '\*\*\*\*\*'.
- Buttons:** 'Save', 'Restore', and 'Help' are located on the right side of the form.
- Header:** 'Quick Setup' is on the top left, and 'Administrator: admin' is on the top right.

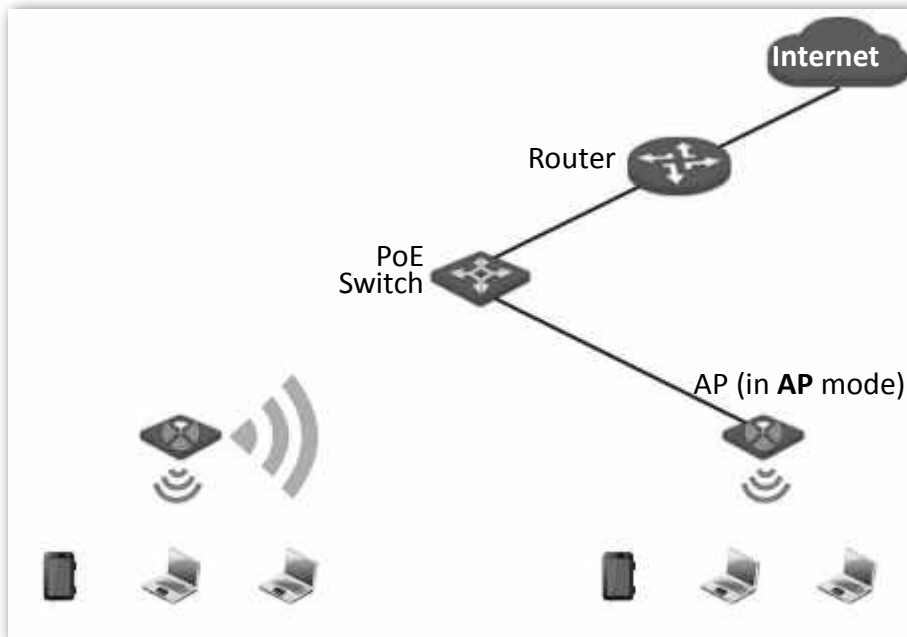
---End

After configuration, you can connect wireless devices to the WiFi network of your AP using the SSID and WiFi password you set.

## 3.2 Client+AP mode

### 3.2.1 Typical network topology

In this mode, the AP extends the existing wireless network by bridging the upstream wireless signals. See the following typical network topology.



### 3.2.2 Getting familiar with Client+AP mode configuration page

To enter the configuration page, set **Working Mode** to **Client+AP**. See the following figure.

The image shows a 'Quick Setup' configuration page. At the top left is the title 'Quick Setup' and at the top right is a help icon '?'. The page contains the following fields and controls:

- Radio Band:** A dropdown menu set to '2.4GHz'.
- Working Mode:** Two radio buttons, 'AP' and 'Client+AP'. The 'Client+AP' button is selected and highlighted with a red box.
- SSID:** A text input field.
- Security Mode:** A dropdown menu set to 'None'.
- Buttons:** 'Refresh', 'Scan', 'Save', and 'Cancel' buttons are located at the bottom.



### Parameter description

Parameter	Description
Radio Band	It is used to select the radio band for configurations.
Working Mode	<p>It specifies the working modes supported by the device.</p> <ul style="list-style-type: none"><li>- <b>AP mode</b> (default mode): This mode is used to deploy wireless networks by connecting the AP to the internet in a wired manner.</li><li>- <b>Client+AP mode</b>: This mode is used to extend the existing wireless network by bridging the upstream wireless signals.</li></ul>
SSID	It specifies the wireless network name of the upstream wireless network you selected.
Security Mode	<p>It specifies the security mode adopted by the upstream wireless network you selected.</p> <p>See <a href="#">Security Mode</a> for details.</p>
Key	It specifies the WiFi password for the upstream wireless network you selected.
Refresh	Used to refresh the scan results.
Scan/Disable	<ul style="list-style-type: none"><li>- <b>Scan</b>: Used to scan nearby available wireless networks. The scan results are displayed on the lower page.</li><li>- <b>Disable</b>: The button only appears after you clicked Scan. It is used to end the scan operation and collapse the scan result.</li></ul>

## 3.2.3 Configuring Client+AP mode

Log in to the web UI of the AP, and choose **Quick Setup** to enter the configuration page first.



- By default, the device works in **AP** mode.
- The following introduces how to set the device into **Client+AP** mode on 2.4 GHz band. Configuration on 5 GHz is identical.
- This device does not support dual-band bridging in Client+AP mode. Enabling Client+AP mode on 2.4 GHz band clears Client+AP configuration (if any) on 5 GHz band. And vice versa.

### Procedure

1. Select **2.4 GHz** from the **Radio Band** drop-down list menu.
2. Set **Working Mode** to **Client+AP**.
3. Click **Scan**. The nearby available radio signals appear on the lower page.



Tip

If the SSID for bridging is not displayed, check if your upstream wireless network is enabled. If not, enable it. Then refresh the scan result.

4. Select the WiFi network to bridge, which is **IP-COM\_Router** in this example.

The device detects and auto-fills **SSID**, **Security Mode**, **Encryption**, and **Algorithm** of the upstream wireless network for you, except the **Key**, which requires you to enter manually.

5. Click **Save** to apply your settings.

Quick Setup

Radio Band: 2.4GHz

Working Mode: ☐ AP ☒ Client+AP

SSID: IP-COM\_Router

Security Mode: WPA-PSK & WPA2-PSK

Encryption Algorithm: ☒ AES ☐ TKIP ☐ TKIP&AES

Key: .....

Click to refresh scan result. ← Refresh Disable → Click to collapse scan result

Save Cancel

Scan result

Select	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
<input checked="" type="radio"/>	IP-COM_Router	D8:32:14:4C:CB:71	20MHz	11	Mixed WPA/WPA2-PSK...	

---End

After the configuration, devices connected to the AP can access the upstream wireless network.

# 4 Internet settings

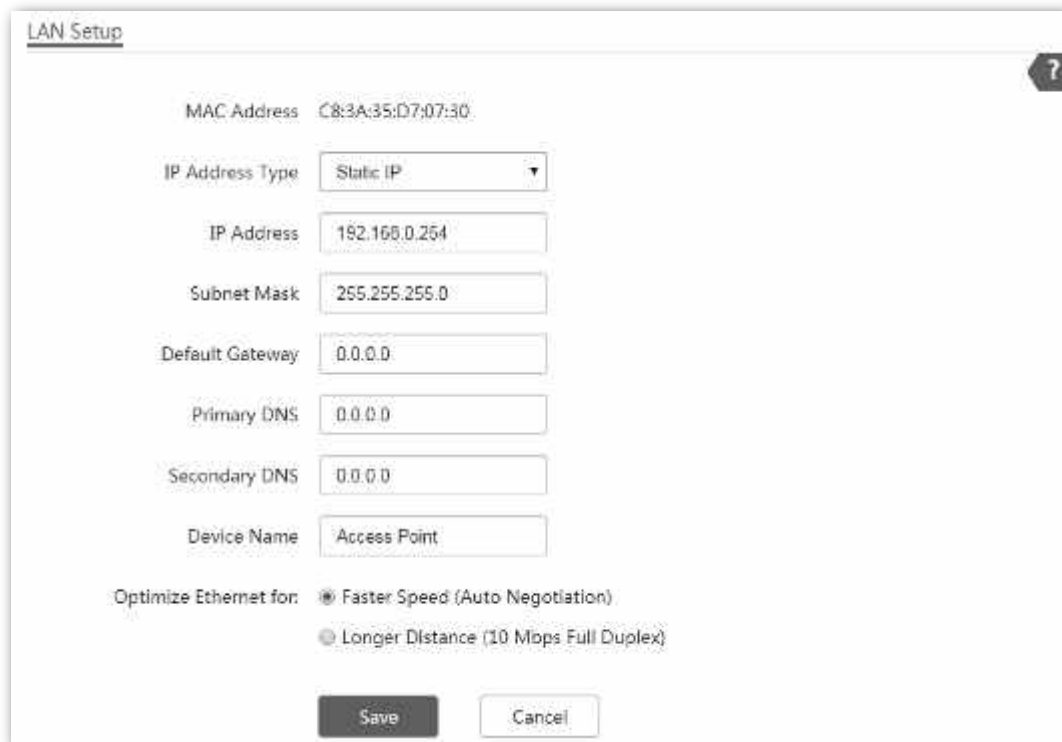
## 4.1 LAN setup

### 4.1.1 Overview

This section introduces how to:

- Modify the IP address obtaining method of the AP.
- Modify device name.
- Modify negotiation mode.

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



The screenshot shows the 'LAN Setup' configuration window. At the top left is the title 'LAN Setup' and a help icon (?) is at the top right. The configuration fields are as follows:



- MAC Address: C8:3A:35:D7:07:30
- IP Address Type: Static IP (dropdown menu)
- 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

At the bottom, there is a section 'Optimize Ethernet for:' with two radio button options:

- ☒ Faster Speed (Auto Negotiation)
- ☐ Longer Distance (10 Mbps Full Duplex)

At the very bottom are two buttons: 'Save' and 'Cancel'.

## Parameter description

Parameter	Description
MAC Address	It specifies the MAC address of the AP's LAN port.
IP Address Type	<p>It specifies IP address obtaining method of the AP.</p> <ul style="list-style-type: none"><li>– <b>Static IP</b> (default): You are required to set related parameters manually.</li><li>– <b>DHCP (Dynamic IP Address)</b>: The AP automatically obtains related parameters from a DHCP server on your LAN network.</li></ul>
IP Address	It specifies the LAN IP address (also the login IP address) of the AP. Default: <b>192.168.0.254</b> .
Subnet Mask	It specifies the subnet mask of the AP. Default: <b>255.255.255.0</b> .
Default Gateway	<p>It specifies the gateway IP address of the AP.</p> <p>Generally, enter the LAN IP address of the router which has internet accessibility into this box.</p>
Primary DNS	<p>It specifies the IP address of the primary DNS server of the AP.</p> <p>If DNS proxy function is supported on your router connected to the internet, you can set the IP address of the primary DNS server to the LAN IP address of your router. Otherwise, enter a correct DNS server IP address.</p>
Secondary DNS	It specifies the IP address of the secondary DNS server of the AP. This parameter is optional.
Device Name	<p>It specifies the name of the AP.</p> <div> Tip</div> <p>For later convenient management, you are recommended to modify each AP's name.</p>
Optimize Ethernet for	<div> Tip</div> <ul style="list-style-type: none"><li>– <b>Faster Speed (Auto Negotiation)</b>: This option features a high data rate but short transmission distance. Generally, we recommend you select this option.</li><li>– <b>Longer Distance (10 Mbps Half Duplex)</b>: This option features long transmission distance but low data rate. Generally, the negotiated speed is 10 Mbps.</li></ul> <p>If the Ethernet cable connecting the Ethernet port of the AP to the peer device is longer than 100 meters, the <b>Longer Distance</b> mode is recommended. In this case, ensure that the peer device adopts auto negotiation option.</p>

## 4.1.2 Configuring the AP to obtain IP address automatically (for multiple APs)

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

### Procedure

1. Select **DHCP (Dynamic IP Address)** from the **IP Address Type** drop-down list menu.  
The IP address-related parameters dimmed and cannot be configured.
2. Click **Save** to apply your settings.

LAN Setup

MAC Address C8:3A:35:D7:07:30

IP Address Type DHCP (Dynamic IP Add ▾)

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

---End

To view the new IP address assigned to the AP, go to the upstream DHCP client list.

### 4.1.3 Configuring the AP to use static IP address (for few APs)

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

#### Procedure

1. Select **Static IP** from the **IP Address Type** drop-down list menu.  
The IP address-related parameters become configurable.
2. Customize required parameters.
3. Click **Save** to apply your settings.

LAN Setup

MAC Address C8:3A:35:D7:07:30

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

---End

After the configuration, if the new IP address of the AP belongs to the same network segment as the IP address of your management computer, you can log in to the web UI of the AP directly using the new IP address. Otherwise, before logging in to the AP's web UI using the new IP address, assign your computer an IP address that belongs to the same network segment as the new IP address.

## 4.2 DHCP server

### 4.2.1 Overview

The AP supports the DHCP server function to assign IP addresses to devices connected to it. By default, this function is disabled. After this function enabled, the following page appears.






Note

If another DHCP server is available in your LAN, ensure that the IP address pool of the AP does not overlap the IP address pool of that DHCP server. Otherwise, IP address conflicts may occur.

#### Parameter description

Parameter	Description
DHCP Server	It specifies whether or not to enable the DHCP server function of the AP. By default, it is disabled.
Start IP Address	It specifies the start IP address of the DHCP server's IP address pool. The default value is <b>192.168.0.100</b> .
End IP Address	It specifies the end IP address of the DHCP server's IP address pool. The default value is <b>192.168.0.200</b> .

 Tip

Parameter	Description
	The <b>End IP address</b> must be greater than the <b>Start IP address</b> .
Subnet Mask	It specifies the subnet mask assigned by the DHCP server to devices. The default value is <b>255.255.255.0</b> .
Gateway Address	<p>It specifies the gateway IP address assigned by the DHCP server to devices. Generally, it is the LAN IP address of the router connected to the internet. The default value is <b>192.168.0.1</b>.</p> <p> Tip</p> <p>Only through a gateway can a LAN device access a server or host which is not in the local network segment. You are recommended to enter a gateway IP address which can access the internet. Otherwise, the device in the LAN network cannot access the internet.</p>
Primary DNS	<p>It specifies the DNS server address provided by your ISP. If you do not know it, please consult your ISP.</p> <p> Tip</p> <p>To enable devices to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.</p>
Secondary DNS	It specifies the second DNS server address (if any) provided by your ISP. This parameter is optional, which indicates you can leave it blank if your ISP does not provide this parameter.
Lease Time	<p>It specifies the validity period of an IP address assigned by the DHCP server to a device. By default, it is <b>1</b> day.</p> <p>When half of the lease time has elapsed, the device sends a DHCP request to the DHCP server to renew the lease time. If the request succeeds, the lease time is extended based on the request. Otherwise, the device sends a request again when 7/8 of the lease time has elapsed. If the request succeeds, the lease time is extended based on the request. Otherwise, the device must request a new IP address from the DHCP server after the lease time expires.</p> <p>You are recommended to retain the default value.</p>

## 4.2.2 Configuring DHCP server of the AP

To access the configuration page, choose **Internet Settings > DHCP Server**.

### Procedure

1. Enable **DHCP Server** function.
2. Customize required parameters.





Tip

- The **End IP Address** must be greater than the **Start IP Address**.
- The **Start IP Address**, **End IP Address**, and **Gateway Address** must belong to the same network segment as that of the LAN IP of the device.

3. Click **Save** to apply your settings.

DHCP Server DHCP Clients

DHCP Server ☒

Start IP Address

End IP Address

Subnet Mask

Gateway Address

Primary DNS

Secondary DNS

Lease Time

---End

## 4.2.3 Viewing DHCP clients

To view DHCP clients and their connection information, choose **Internet Settings > DHCP Server**, and click the **DHCP Clients** tab. See the following figure.

DHCP Server DHCP Clients

**DHCP client list**

ID	Host Name	IP Address	MAC Address	Lease Time
1	Honor_9-2b0d9d81e4...	192.168.1.147	54-B1-21:56:62:45	23hrs 57min 55sec

10 in total/Page 1 in total

# 5 Wireless

## 5.1 SSID

### 5.1.1 Overview

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

To access the configuration page, choose **Wireless > SSID**.

Administrator: admin

2.4 GHz SSID Settings

5 GHz SSID Settings

SSID

IP-COM\_888888

Save

Enable

☒ Enable ☐ Disable

Restore

Broadcast SSID

☒ Enable ☐ Disable

Help

Isolate Client

☒ Enable ☐ Disable

WMF

☒ Enable ☐ Disable

Suppress Broadcast Probe Response

☒ Enable ☐ Disable

Max. Number of Clients

48

(Range: 1 to 128)

SSID

IP-COM\_888888

Chinese SSID Encoding



UTF-8



Security Mode

None

#### Parameter description

Parameter	Description
SSID	Select one SSID from the drop-down list menu.

Parameter	Description
	 Tip <p>The AP allows you to enable <b>8 SSIDs</b> on <b>2.4 GHz</b> band, and <b>4 SSIDs</b> on <b>5 GHz</b> band.</p>
Enable	Used to enable or disable the wireless network you selected.
Broadcast SSID	<ul style="list-style-type: none"> <li>- <b>Enable:</b> Nearby wireless clients can detect the SSID.</li> <li>- <b>Disable:</b> Nearby wireless clients cannot detect the SSID, and you need to enter the SSID manually on the wireless client to access the wireless network.</li> </ul>
Isolate Client	This parameter implements a function similar to the VLAN function for wired networks. It isolates the wireless devices connected to the same WiFi network, so that the wireless devices can access only the wired network connected to the AP. You can apply this function to hotspot setup in public spaces, such as hotels and airports to improve network security.
WMF	<p>The number of wireless devices keeps increasing currently, but wired and wireless bandwidth resources are limited. Therefore, the multicast technology, which enables single-point data transmission and multi-point data reception, has been widely used in networks in order to reduce bandwidth requirements and prevent network congestion.</p> <p>Nevertheless, if a large number of devices are connected to a wireless interface of a WiFi network and multicast data is intended for only one of the devices, the data is still sent to all the devices, which increases unnecessary wireless resource usage and may lead to wireless channel congestion. In addition, multicast stream forwarding over an 802.11 network is not secure, either.</p> <p>The WMF function of the AP converts multicast traffic into unicast traffic and forwards the traffic to the multicast traffic destination in the WiFi network, helping save wireless resources, ensuring reliable transmission, and reducing delays.</p>
Suppress Broadcast Probe Response	If enabled, this device does not respond to the requests without an SSID, saving wireless resources.
Max. Number of Clients	<p>This parameter specifies the maximum number of devices that can connect to the WiFi network corresponding to an SSID. If the number is reached, the WiFi network rejects new connection requests from devices. This limit helps balance load among SSIDs.</p>  Tip <p>The AP supports <b>128</b> clients at most. That is to say, clients connected to all the enabled wireless networks of the AP cannot exceed 128. If you enable multiple SSIDs, plan your maximum number of clients to each SSID first.</p>
Chinese SSID Encoding	<p>It specifies the character encoding format.</p> <p>Available options include <b>GB2312</b> and <b>UTF-8</b>.</p>

Parameter	Description
	 Tip A proper encoding format lets the SSID containing Chinese characters be displayed normally across devices.
Security Mode	<p>It specifies the security modes supported by the AP, including:</p> <ul style="list-style-type: none"><li>- <b>None</b>: This wireless network is open. The security level is the lowest.</li><li>- <b>WEP</b>: Wired Equivalent Privacy. The security level is very low.</li><li>- <b>WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK</b>: Applicable to most scenarios.</li><li>- <b>WPA and WPA2</b>: This mode provides highest security level. It use 802.1 x RADUIS to encrypt and is applicable to enterprises.</li></ul>  Tip See <a href="#">Security Mode</a> for details.

## Security Mode

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

The AP supports various security modes for network encryption, including **None**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **Mixed WPA/WPA2-PSK**, and **WPA/WPA2**.

### ■ None

It indicates that any wireless device can connect to the WiFi network. This option is not recommended because it leads to network insecurity.

### ■ WEP

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

### ■ 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 WiFi networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all devices 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.

#### ■ WPA and 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 devices and generate data encryption-oriented root keys. WPA and WPA2 use the root keys to replace the pre-shared keys that set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK.

WPA and WPA2 uses 802.1x to authenticate devices and the login information of a device is managed by the device. This effectively reduces the probability of information leakage. In addition, each time a device 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 device, which makes it difficult for attackers to obtain the key. These features of WPA and WPA2 security modes help increase network security significantly, making WPA and WPA2 the preferred security modes of WiFi networks that require high security.

## 5.1.2 Modifying SSID-related parameters

To enter the configuration page, choose **Wireless > SSID** first.

### Procedure



- The following takes configuration on 2.4 GHz band for example. Configuration on 5 GHz is identical.
- The following introduces how to modify parameters on this page. Modify them based on your actual requirements.

1. Select the SSID from the **SSID** drop-down list menu.
2. Set **Status** to **Enable**.
3. (Optional) Enable **Broadcast SSID**, **Isolate Client**, **Isolate SSID**, **WMF**, and modify the number of client that can connect to this specific SSID in the **Max. Number of Clients** box.



Tip

- The AP supports **128** clients at most. That is to say, clients connected to all the enabled wireless networks of the AP cannot exceed 128. If you enable multiple SSIDs, plan your maximum number of clients to each SSID first.
- The AP allows you to enable **8** SSIDs on **2.4 GHz** band, and **4** SSIDs on **5 GHz**.

4. (Optional) Customize SSID and security-related parameters as required.
  - **SSID:** Modify the default one if necessary.
  - **Chinese SSID Encoding:** A proper encoding format lets the SSID containing Chinese characters be displayed normally across devices.
  - **Security Mode:** Choose a security mode and configure related parameters.
5. Click **Save** to apply your settings.

2.4 GHz 5 GHz

SSID: Test\_01

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: Test\_01

Chinese SSID Encoding: UTF-8

Security Mode: Mixed WAP/WPA2-PSK

Encryption Algorithm: ☒ AES ☐ TKIP ☐ TKIP&AES

Key: .....

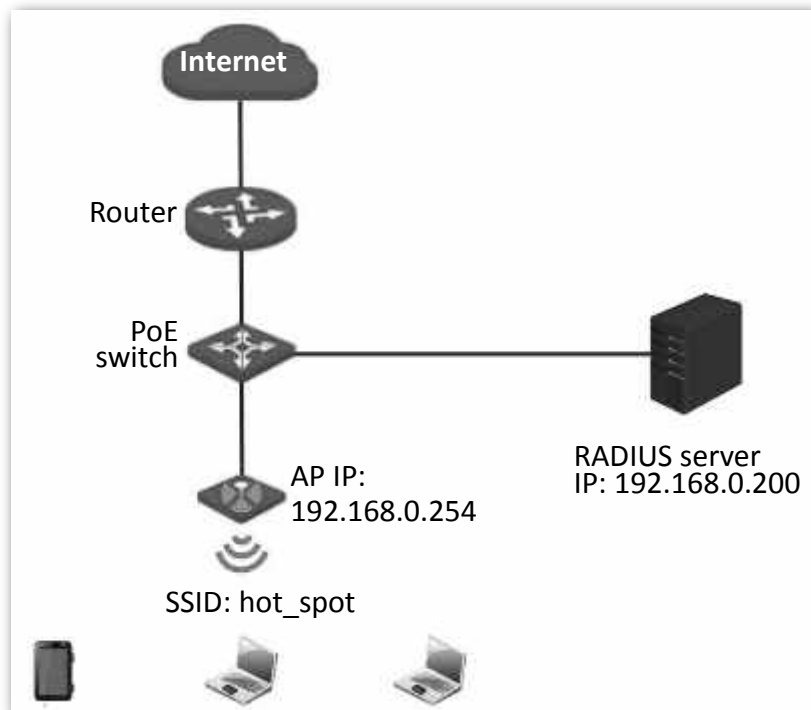
Key Update Interval: 0 Second (Range: 60 to 99999. 0 indicates no upgrade)

Save Cancel

---End

### 5.1.3 Example of configuring a WiFi network encrypted by WPA or WPA2

#### Network topology



#### Configuration description

Configuring a WiFi network encrypted by WPA or WPA2 involves operations across various devices. This guide will walk you through the configuration step by step.

The following table summarizes the overall steps. Get yourself familiar with the whole process before you start.

Step	Task	Description
1	Configure the AP.	Select the SSID you want to implement the RADIUS authentication, and enable it. Modify the SSID as required. Then set the security mode to WPA2 and enter the RADIUS server-related parameters.
2	Create RADIUS client.	Create a RADIUS client first, and then create a remote access policy.
3	Configure wireless network information on the wireless client.	Add the wireless network enabled with WPA or WPA2 of the AP manually, and configure its security settings.

## Procedure

### 1. Configure the AP.



In this case, we assume that you have installed and configured a RADIUS server in your company, and have obtained the following information:

- **RADIUS Server:** IP address or domain name of the RADIUS server, which is **192.168.0.200** in this example.
- **RADIUS Port:** Port number used for authentication, which is **1812** in this example
- **RADIUS Password:** Password used for authentication which is **12345678** in this example.

- (1) Select an SSID from the **SSID** drop-down list menu, and set the **Status** to **Enable**.
- (2) Modify the **SSID** to **hot\_spot**.
- (3) Select **WPA2** from the **Security Mode** drop-down list menu. The RADIUS-related parameters appear.
- (4) Enter your **RADIUS Server**, **RADIUS Port**, and **RADIUS Password**. Parameters on the following figure are only for examples.
- (5) Set **Encryption Algorithm** to **AES**.
- (6) Click **Save** to apply your settings.



SSID	Test_01	
Status	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

Broadcast SSID	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Isolate Client	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Isolate SSID	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
WMF	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

Max. Number of Clients	48	(Range: 1 to 128)
------------------------	----	-------------------

SSID	hot_spot	
Chinese SSID Encoding	UTF-8	

Security Mode	WPA2	
RADIUS Server	192.168.0.200	
RADIUS Port	1812	(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)
---------------------	---	---

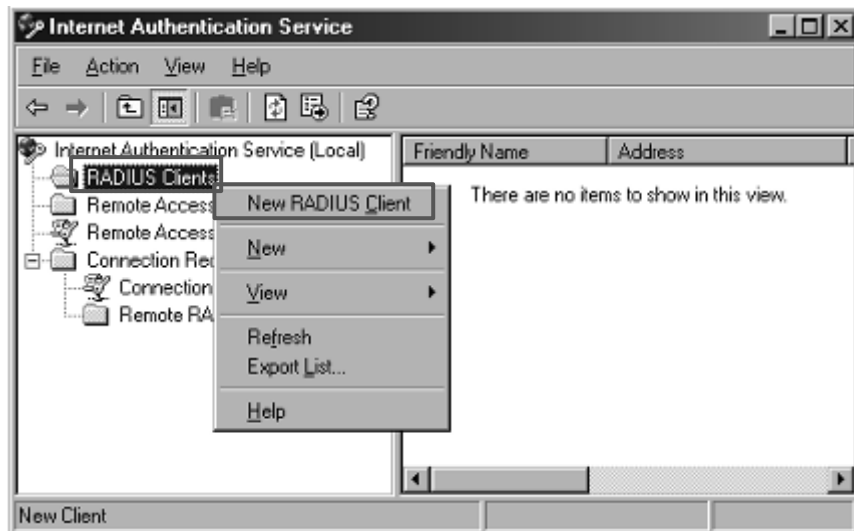
Save

Cancel

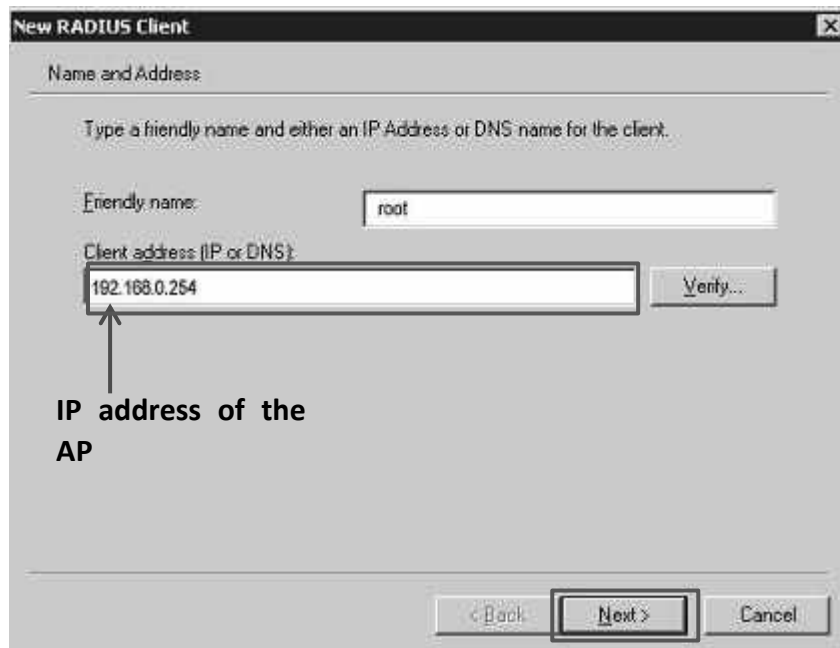
## 2. Configure RADIUS client (Example: Windows 2003)

### (1) Configure a RADIUS client.

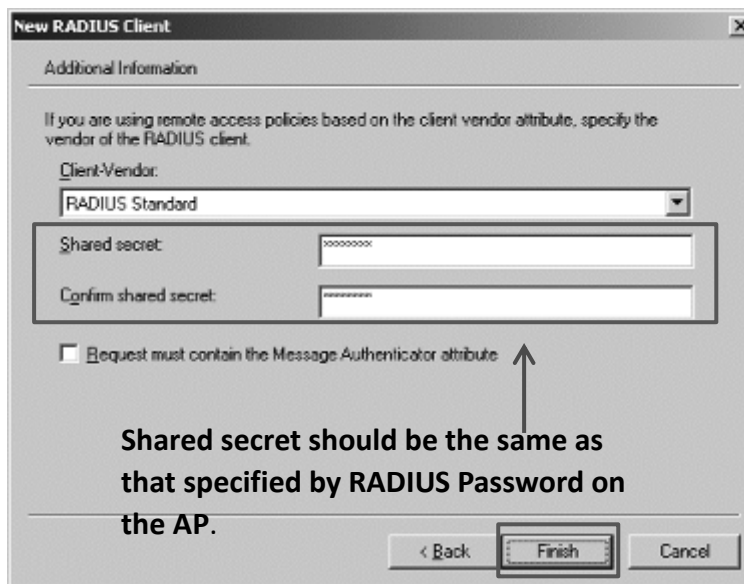
In the **Computer Management** dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.



Enter a RADIUS client name (device name of the AP is recommended) and the IP address of the AP, and click **Next**.



Enter **12345678** in the **Shared secret** and **Confirm shared secret** text boxes, and click **Finish**.

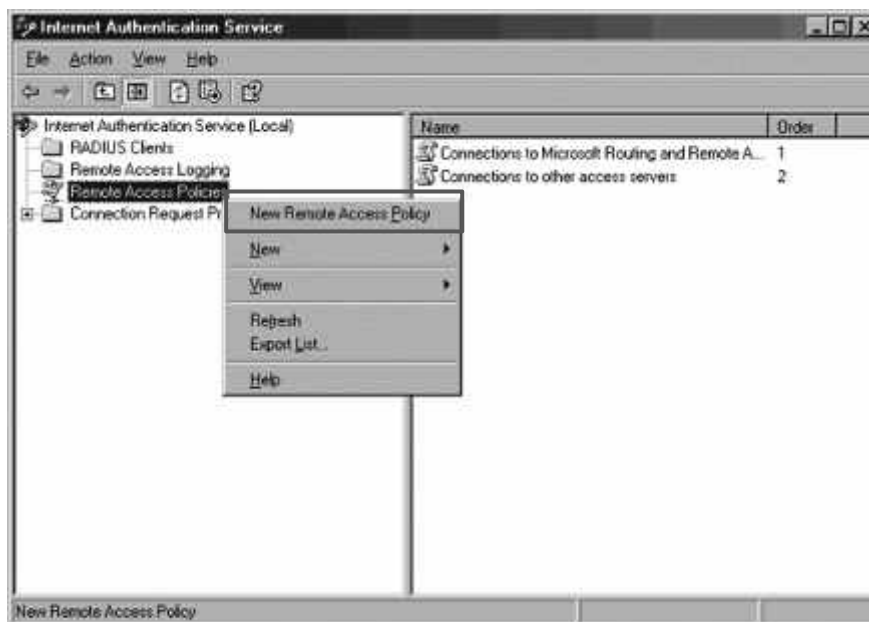


The 'New RADIUS Client' dialog box is shown. It has a title bar 'New RADIUS Client' and a close button. The main area is titled 'Additional Information'. Below this, there is a text box for 'Client-Vendor' with a dropdown menu showing 'RADIUS Standard'. Below that are two text boxes for 'Shared secret' and 'Confirm shared secret', both containing masked characters. Below these is a checkbox labeled 'Request must contain the Message Authenticator attribute'. At the bottom are three buttons: '< Back', 'Finish', and 'Cancel'. An arrow points from the 'Finish' button to the text below.

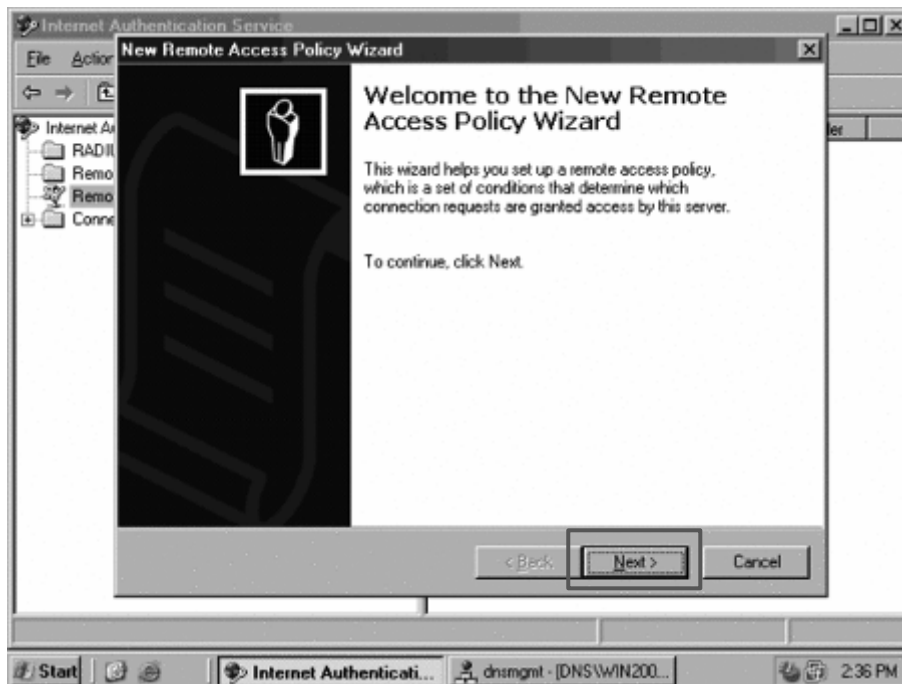
Shared secret should be the same as that specified by RADIUS Password on the AP.

- (2) Configure a remote access policy.

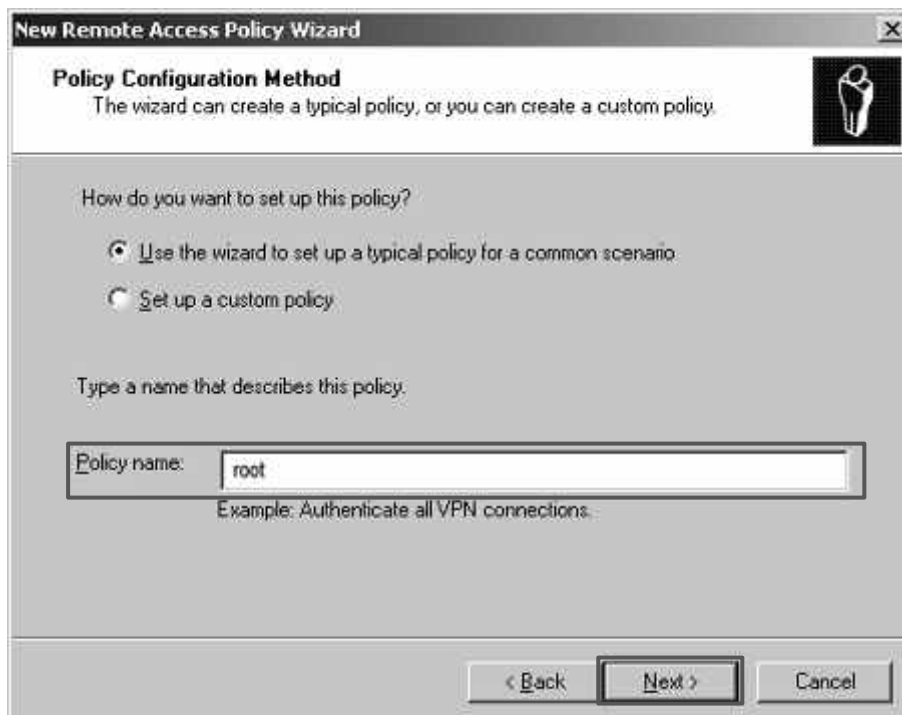
Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



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



Enter a policy name and click **Next**.



Select **Ethernet** and click **Next**.



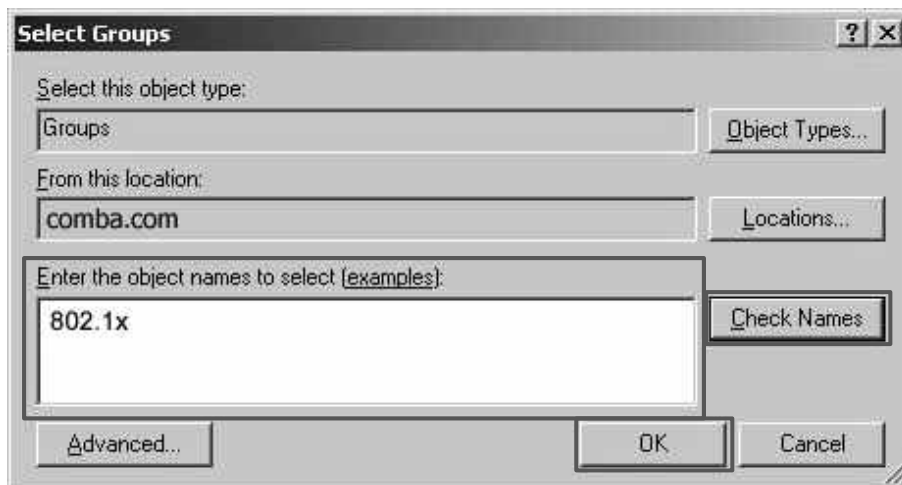
The screenshot shows the 'New Remote Access Policy Wizard' window, specifically the 'Access Method' step. The title bar reads 'New Remote Access Policy Wizard'. Below the title bar, the section 'Access Method' is displayed with a subtext: 'Policy conditions are based on the method used to gain access to the network.' To the right of this text is a small icon of a person. The main area contains the instruction 'Select the method of access for which you want to create a policy.' followed by three radio button options: 'VPN' (with subtext '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' (with subtext 'Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.'), and 'Wireless' (with subtext 'Use for wireless LAN connections only.'). The 'Ethernet' option is selected (indicated by a filled radio button) and is enclosed in a rectangular box; its subtext is 'Use for Ethernet connections, such as connections that use a switch.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a rectangular box.

Select **Group** and click **Add**.

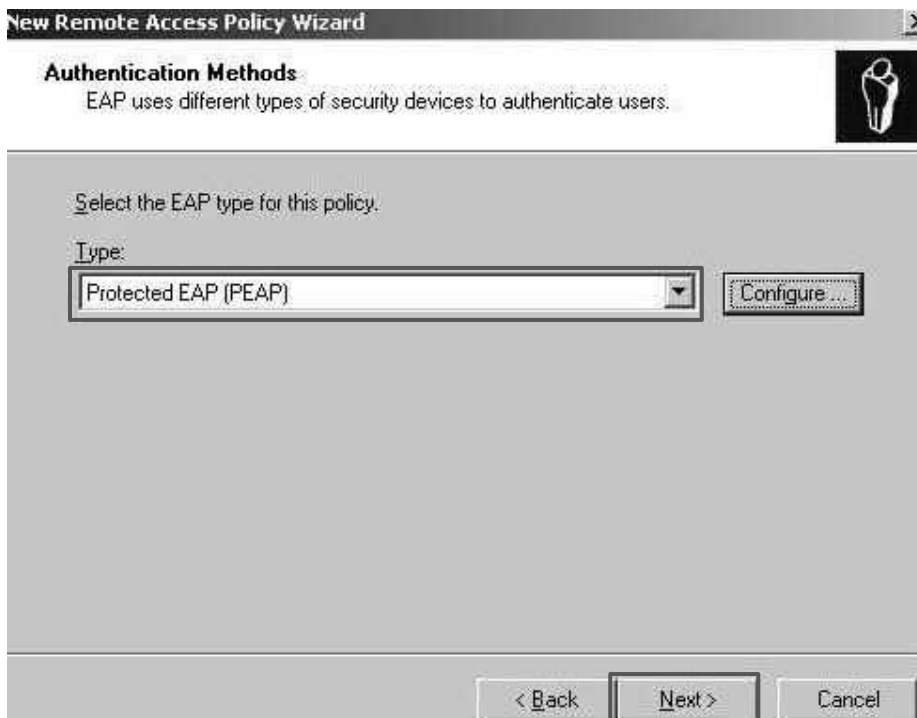


The screenshot shows the 'New Remote Access Policy Wizard' window, specifically the 'User or Group Access' step. The title bar reads 'New Remote Access Policy Wizard'. Below the title bar, the section 'User or Group Access' is displayed with a subtext: 'You can grant access to individual users, or you can grant access to selected groups.' To the right of this text is a small icon of a person. The main area contains the instruction 'Grant access based on the following:' followed by two radio button options: 'User' (with subtext 'User access permissions are specified in the user account.') and 'Group' (with subtext 'Individual user permissions override group permissions.'). The 'Group' option is selected (indicated by a filled radio button) and is enclosed in a rectangular box. Below the 'Group' option is a text field labeled 'Group name:' which is currently empty. To the right of this text field are two buttons: 'Add...' and 'Remove'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a rectangular box.

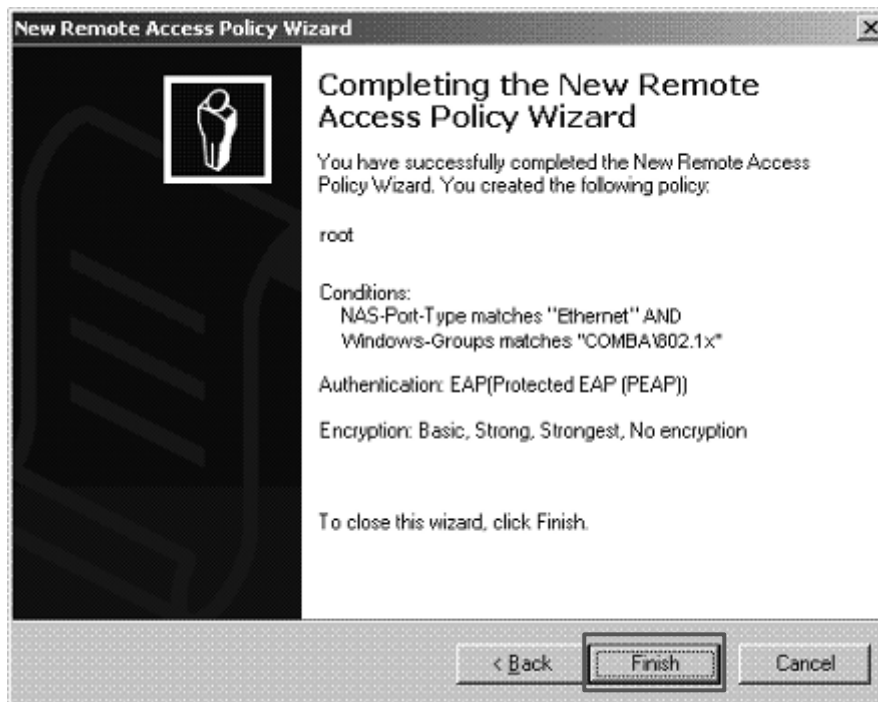
Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



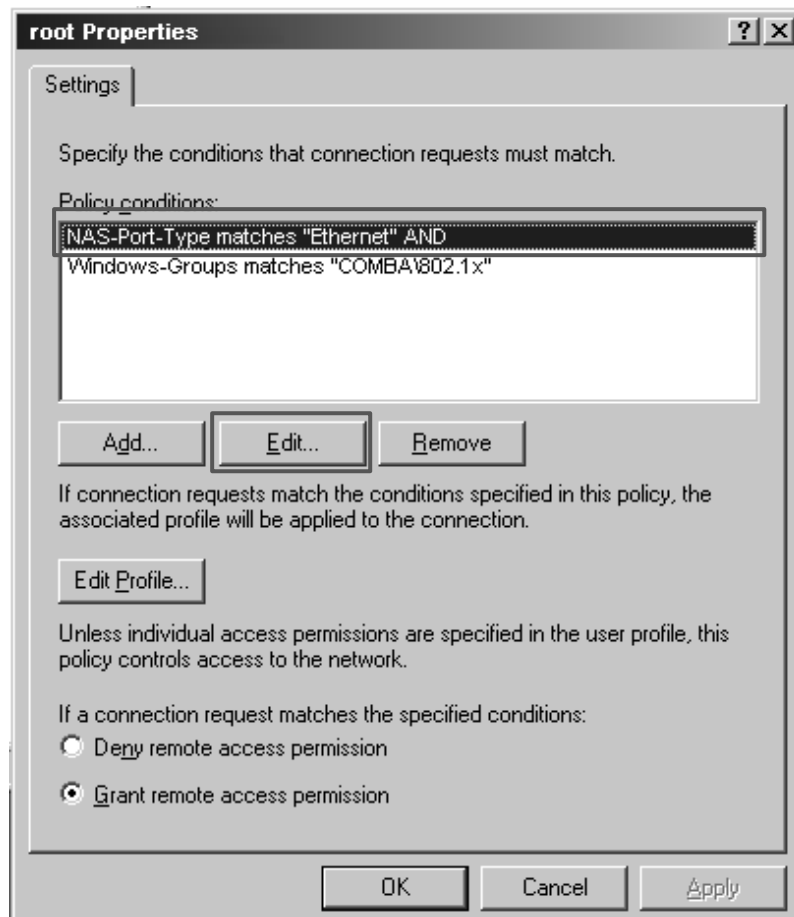
Select **Protected EAP (PEAP)** and click **Next**.



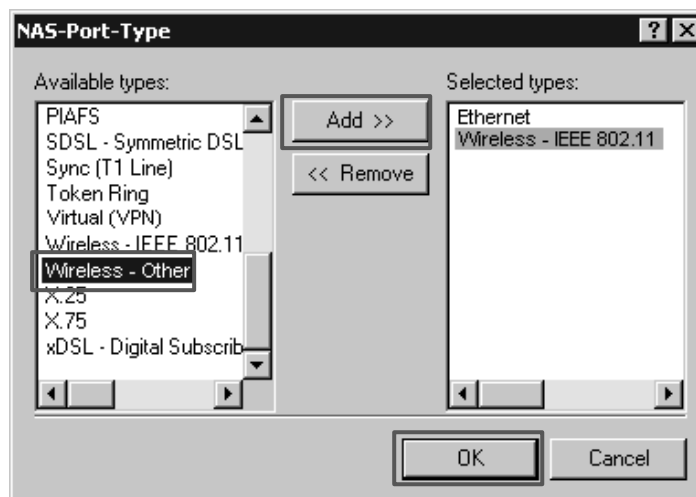
Click **Finish**. The remote access policy is created.



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

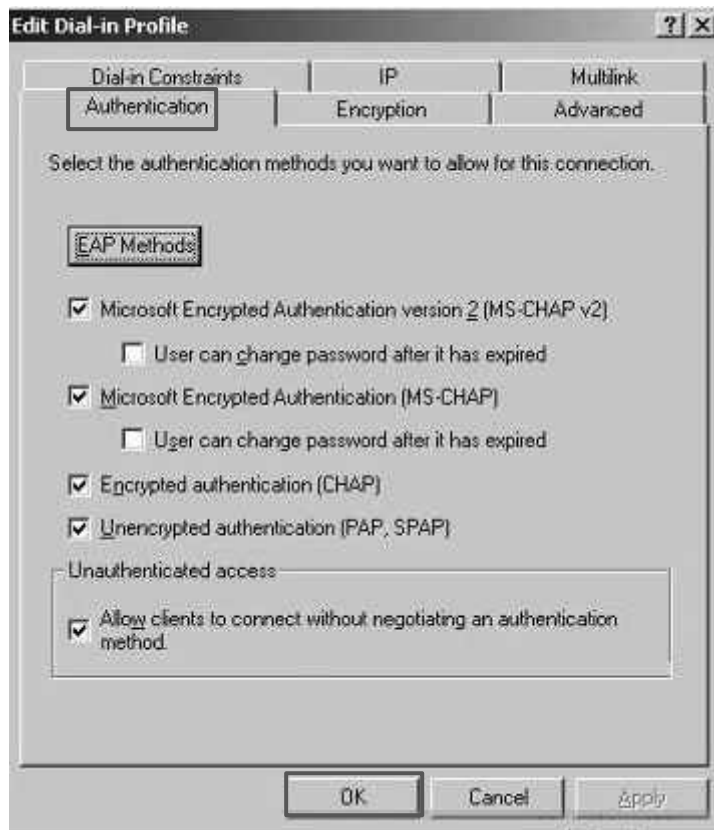


Select **Wireless – Other**, click **Add**, and click **OK**.



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





When a message appears, click **No**.

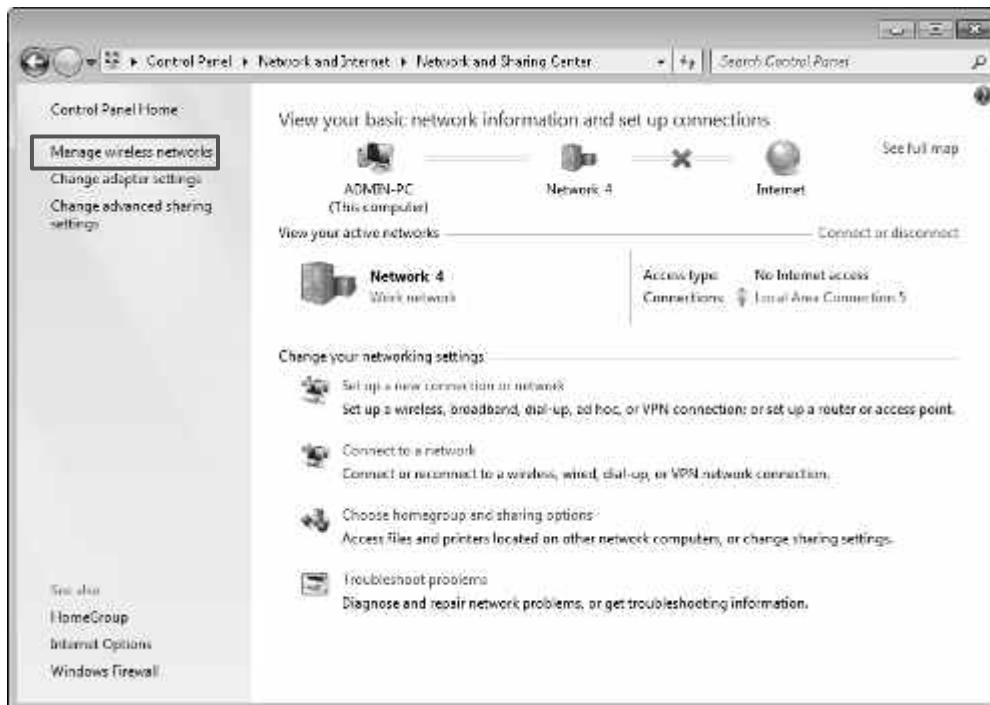
- (3) Configure user information.

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

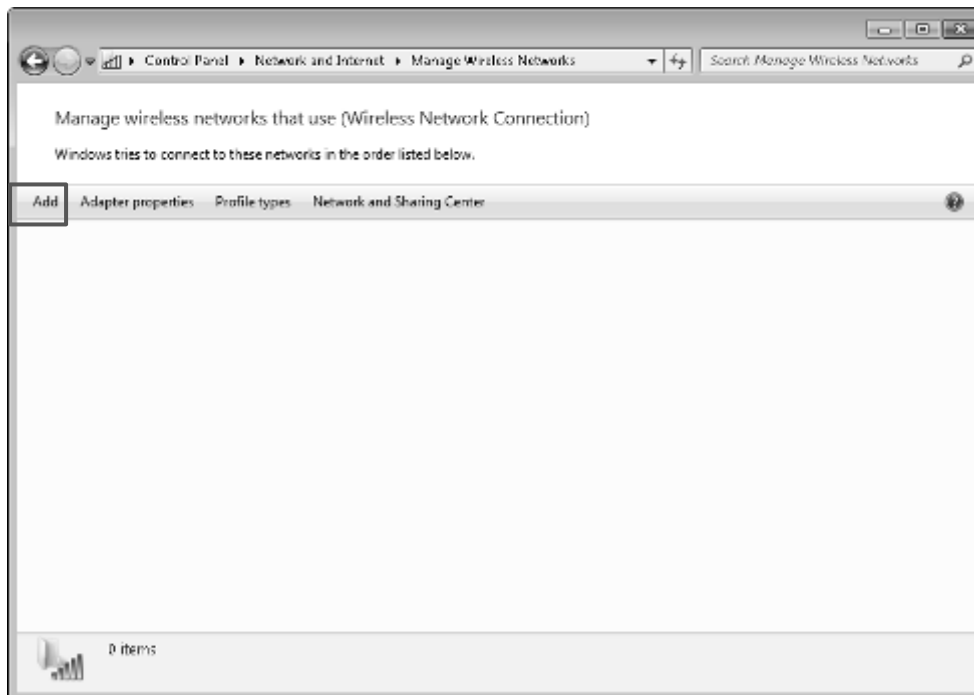
---End

### 3. Configure wireless settings on the wireless client (Example: Windows 7)

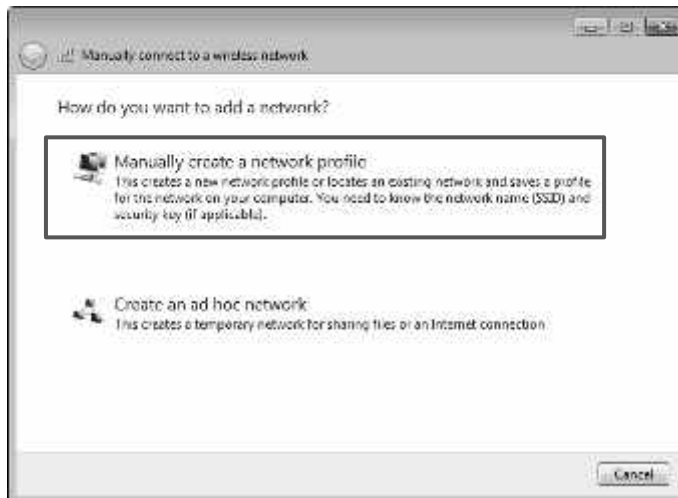
Choose **Start > Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



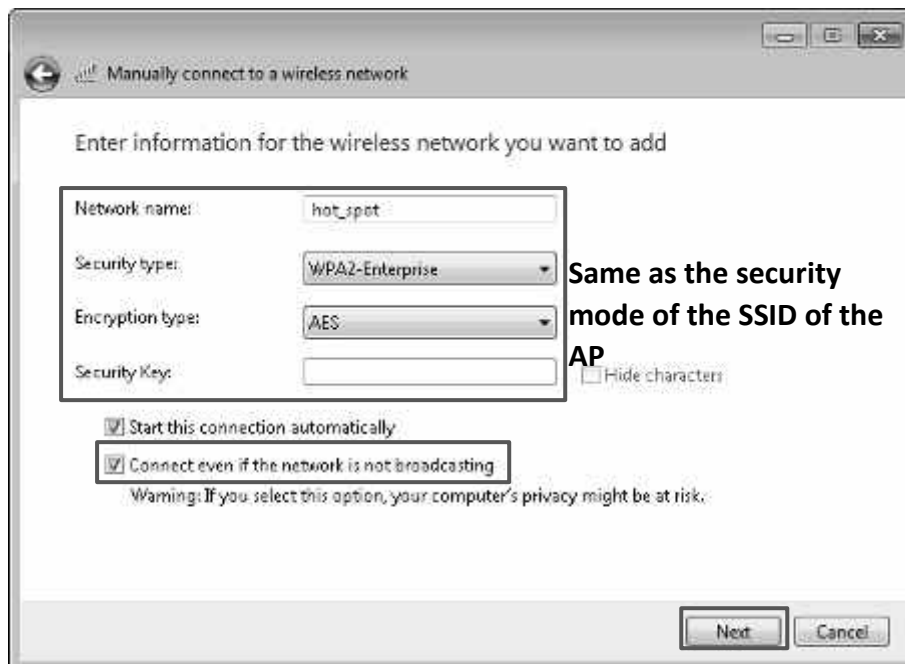
Click **Add**.



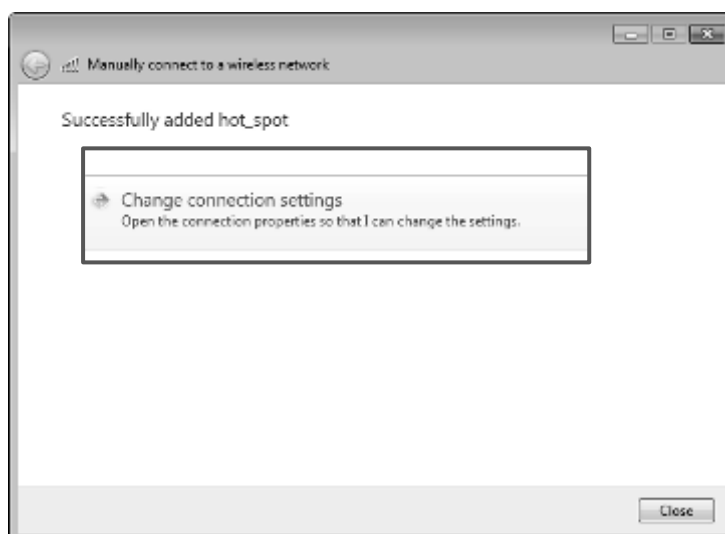
Click **Manually create a network profile**.



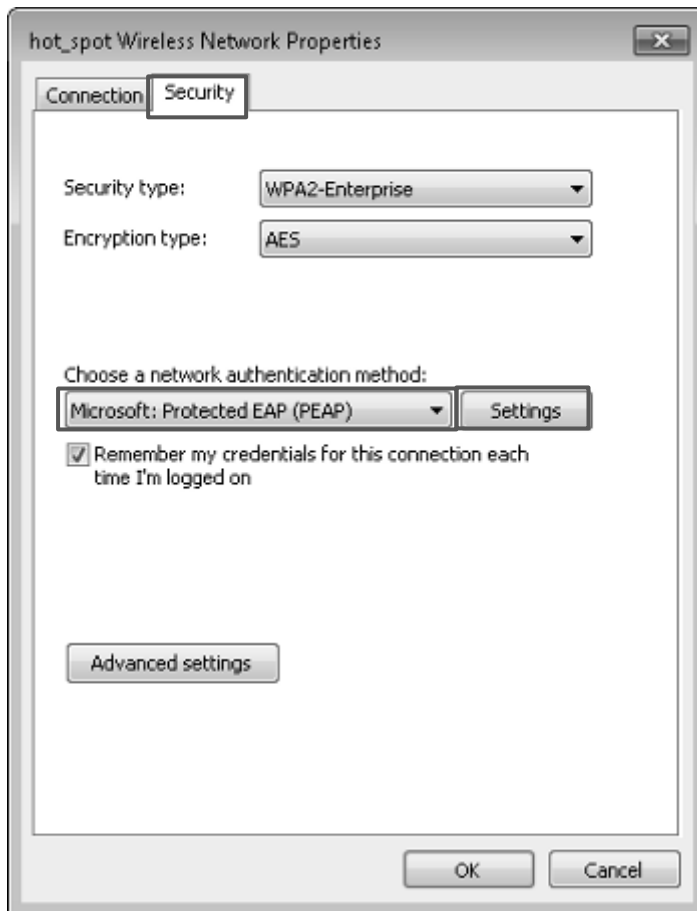
Enter WiFi network information, select **Connect even if the network is not broadcasting**, and click **Next**.



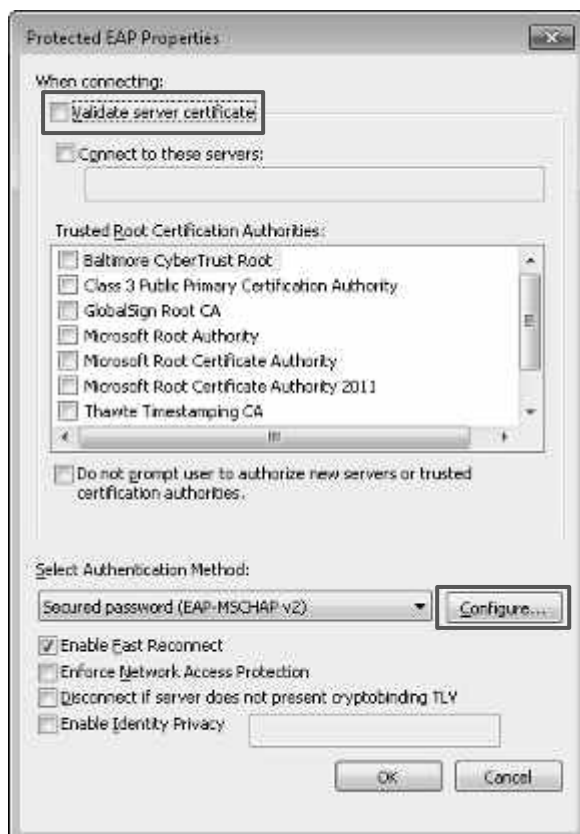
Click **Change connection settings**.



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



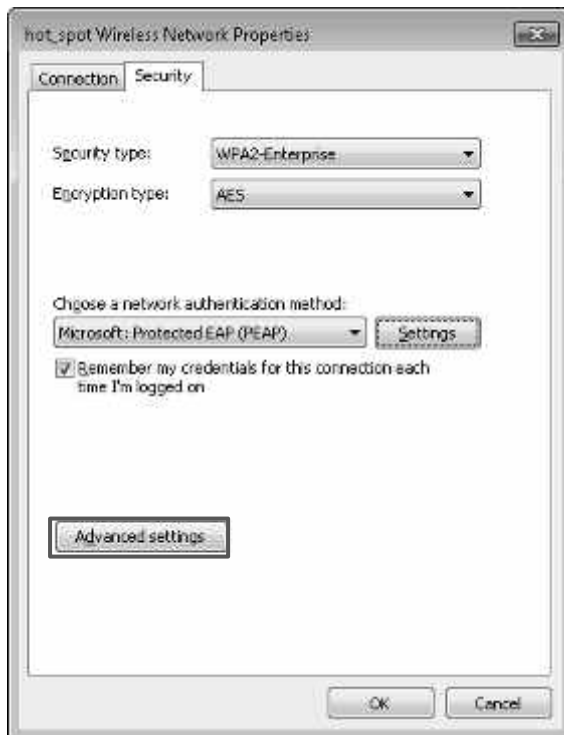
Deselect **Validate server certificate** and click **Configure**.



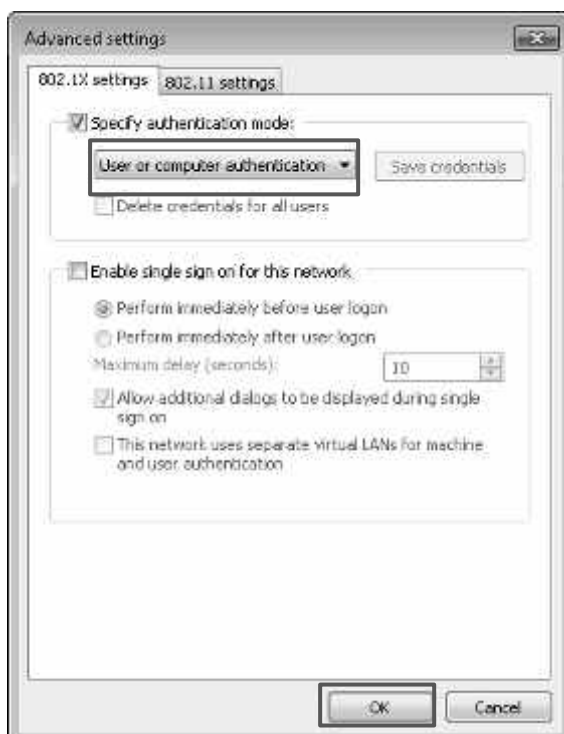
Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



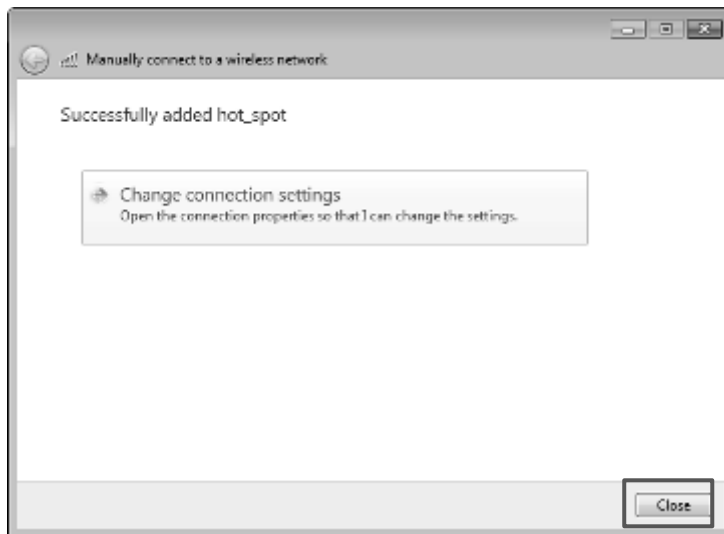
Click **Advanced settings**.



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



Click **Close**.



---End

## Verification

Click the network icon in the lower-right corner of the desktop and choose the WiFi network of the AP, which is **hot\_spot** in this example.



In the **Windows Security** dialog box that appears, enter the user name and password set on the RADIUS server and click **OK**.





## 5.2 RF settings

### 5.2.1 Overview

RF (Radio Frequency) settings allow you to configure advanced settings about the AP, such as channel, power, short GI etc.

To enter the configuration page, choose **Wireless > RF Settings**.

2.4 GHz 5 GHz

Wireless Network ☒

Country/Region China

Network Mode 11b/g/n

Channel Auto

Channel Bandwidth 20MHz

Lock Channel ☒

Transmit Power  10dBm 23dBm

Lock Power ☒


Preamble ☒ Long Preamble ☐ Short Preamble

Short GI ☒ Enable ☐ Disable

Suppress Broadcast Probe Response ☐ Enable ☒ Disable

Save Cancel

#### Parameter description

Parameter	Description
Wireless Network	It specifies whether to enable the radio function of the AP.
Country/Region	It specifies the country or region where the AP is used.  <b>Note</b> It is the installer's responsibility to comply with channel regulations of the country or region.

Parameter	Description
Network Mode	<p>It specifies the wireless network mode (also called 802.11 mode, radio mode, or wireless mode) of the AP. A proper network mode enables the clients to get the maximum transfer rate and compatibility.</p> <p>Available options for <b>2.4 GHz</b> band: <b>11b</b>, <b>11g</b>, <b>11b/g</b>, and <b>11b/g/n</b> (default).</p> <p>Available options for <b>5 GHz</b> band: <b>11a</b>, <b>11ac</b> (default), and <b>11a/n</b> mixed.</p> <p>You are recommended to keep the default settings.</p>
Channel	<p>It specifies the operating channel of the AP. To configure this parameter, deselect <b>Lock Channel</b>.</p> <p><b>Auto</b> indicates that this device automatically changes to a channel rarely used in the ambient environment to prevent interference.</p>
Channel Bandwidth	<p>It specifies the wireless channel bandwidth of the AP.</p> <p>Available options for <b>2.4 GHz</b> band: <b>20MHz</b> (default), <b>40MHz</b>, and <b>20/40MHz</b>.</p> <p>Available options for <b>5 GHz</b> band: <b>20MHz</b>, <b>40MHz</b>, and <b>80 MHz</b> (default).</p>
Extension Channel	<p>It specifies the wireless extension channel of the AP.</p> <p>Available only when <b>Channel Bandwidth</b> is set to <b>40MHz</b>, and <b>20/40MHz</b> on <b>2.4 GHz</b> band.</p>
Lock Channel	<p>If selected, <b>Country/Region</b>, <b>Network Mode</b>, and channel-related parameters (including <b>Channel Bandwidth</b> and <b>Extension Channel</b>) become dim and cannot be modified. By default, it is selected.</p>
Transmit Power	<p>Transmit power of this device.</p> <p>A higher value leads to wider WiFi coverage. However, decreasing the value properly increases performance and security of the wireless network.</p> <p>To adjust it, deselect <b>Lock Power</b> first.</p>
Lock Power	<p>If selected, the <b>Transmit Power</b> cannot be adjusted.</p> <p>By default, it is selected.</p>
Preamble	<p>It specifies a group of bits located at the beginning of a packet, according to which the receiver of the packet can perform synchronization and prepare for receiving data.</p> <p>By default, the <b>Long Preamble</b> option is selected for compatibility with old network adopters installed on wireless devices.</p>
Short GI	<p>Short guard interval for preventing data block interference.</p> <p>Propagation delays may occur on the receiver side due to factors such as multipath wireless signal transmission. If a data block is transmitted at an overly high speed, it may interfere with the previous data block. The short GI helps prevent such interference. Enabling the short GI can yield a 10% improvement in wireless data throughput.</p>
Suppress Broadcast Probe Response	<p>Whether or not to suppress the broadcast probe response.</p> <p>If enabled, this device does not respond to the requests without an SSID, saving wireless resources.</p>

## 5.2.2 Configuring RF settings

To enter the configuration page, choose **Wireless > RF Settings** first.

By default, dimmed parameters, including channel-related parameters and transmit power cannot be modified or adjusted. To modify or adjust these parameters, you need to deselect **Lock Channel** and/or **Lock Power** first.

Modify or adjust these parameters according to your actual requirement.

## 5.3 RF optimization

### 5.3.1 Overview

The AP allows you to configure advanced settings about radio frequency to optimize the AP performance. Please modify these parameters under the professional guidance.

To enter the configuration page, choose **Wireless > RF Settings**.

2.4 GHz 5 GHz

Beacon Interval  ms (Range: 40 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


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

#### Parameter description

Parameter	Description
Beacon Interval	<p>It specifies the interval for transmitting the Beacon frame.</p> <p>The Beacon frame is transmitted at the specified interval to announce the presence of a wireless network. Generally, a smaller interval enables wireless devices to connect to the AP more quickly, while a larger interval ensures higher data transmission speed for the AP.</p>

Parameter	Description
Fragment Threshold	<p>It specifies the threshold of a fragment. Unit: <b>byte</b>.</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 an environment of high error rate, you can reduce the threshold to enable the AP to resend only the fragments that have not been sent successfully, so as to increase the frame throughput.</p> <p>In an environment without interference, you can increase the threshold to reduce the number of acknowledgement times, so as to increase the frame throughput.</p>
RTS Threshold	<p>It specifies the frame length threshold for triggering the RTS/CTS mechanism. Unit: <b>byte</b>.</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 WiFi network to recover from conflicts quicker. For a WiFi network with high user density, you can reduce this threshold for reducing conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.</p>
Signal Transmission	<ul style="list-style-type: none"> <li>- <b>Coverage-oriented</b>: This mode broadens WiFi coverage of APs, and is usually used in scenarios deployed with fewer APs, such as offices, warehouses, and hospitals.</li> <li>- <b>Capacity-oriented</b>: 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.</li> </ul>
DTIM Interval	<p>It specifies the interval for transmitting the Delivery Traffic Indication Message (DTIM) frame. Unit: <b>Beacon</b>.</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 <b>DTIM Interval</b> is set to <b>1</b>, the AP transmits all cached frames after each beacon frame is transmitted.</p>
RSSI Threshold	<p>Set a minimum strength of received signals acceptable to the AP. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to the AP.</p> <p>If there are multiple APs, an appropriate <b>RSSI Threshold</b> ensures that wireless devices can connect to the AP' WiFi networks with strong signals.</p>
Prioritize 5 GHz	<p>If enabled, devices that support 5 GHz band choose to connect the AP's 5 GHz WiFi network first. Otherwise, they randomly connect to 2.4GHz or 5 GHz WiFi network. This option is available on the <b>5 GHz</b> configuration page.</p> <p> <b>Tip</b></p> <p>The default RSSI threshold to enable this function is <b>-80</b> dBm. You can adjust the</p>

Parameter	Description
	threshold by customizing the <b>Prioritize 5 GHz Threshold</b> parameter.
Prioritize 5 GHz Threshold	<p>It specifies the RSSI threshold value to trigger the <b>Prioritize 5 GHz</b> function. The default value is <b>-80 dBm</b>.</p> <p>You are recommended to keep the default settings.</p>
Air Interface Scheduling	<p>It specifies whether to enable the air interface scheduling function.</p> <p>This function allows all clients to transmit data for the same duration. If a client transmits data at a low speed and does not finish data transmission within the duration, it can continue transmitting data only in its next data transmission duration. This prevents some slow clients from occupying excessive airtime resources, so as to improve the overall AP efficiency and effectively ensure AP connections for a larger number of clients and greater throughputs.</p>
Anti-interference Mode	<p>Select an interference mitigation mode for your AP.</p> <p>Available options include: <b>0 (Disable)</b>, <b>1 (Suppress weak interference)</b>, <b>2 (Suppress moderate interference)</b>, and <b>3 (Suppress critical interference)</b>.</p>
APSD	<p>Automatic Power Save Delivery.</p> <p>APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.</p>
MU-MIMO	<p>Multi-User Multiple-Input Multiple-Output.</p> <p>If enabled, AP can communicate with multiple users concurrently, avoiding WiFi network congestion and improving communication. This option is available on the <b>5 GHz</b> configuration page.</p>
Client Timeout Interval	<p>It specifies the maximum period before a WiFi client is disconnected from the AP if the client exchanges no data with the AP. When data is exchanged within the period, countdown stops.</p>
Mandatory Rate	<p>It specifies the basic rate sets for normal operation of the AP. The clients can connect to the AP only when they meet the basic rate required by the AP.</p> <p>You can adjust the mandatory rates to deny clients with low rate to improve user experience.</p>
Optional Rate	<p>It specifies the additional speed sets supported by the AP. The clients meeting the basic requirement can connect to the AP with higher rate.</p> <p>You can adjust the optional rates to deny clients with low rate to improve user experience.</p>

## 5.3.2 Modifying radio optimization settings



Note

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

To enter the configuration page, choose **Wireless > RF Optimization** first.



The following takes configuration on 2.4 GHz band for example. Configuration on 5 GHz is identical.

---

#### **Procedure**

1. Locate and modify the parameters as required.
2. Click **Save** to apply your settings.

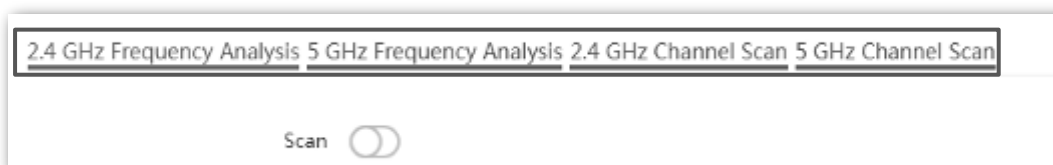
---End



## 5.4 Frequency analysis

This section introduces how to evaluate signal interference in ambient environment. You can use the analysis result to help you configure the AP for best performance.

This module consists of **Frequency Analysis** and **Channel Scan**. Click the corresponding tab to enter the page.



### 5.4.1 Viewing frequency analysis

From the intuitive result, you can read how many wireless networks (total SSID) use the same channel. See the following figure.

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

Scan ☐ Rescan

Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
Total SSID:	24	2	2	6	3	20	6	4	6	9	22	0	3
Channel Usage (%)	93	15	15	35	19	80	35	24	34	51	87	5	19



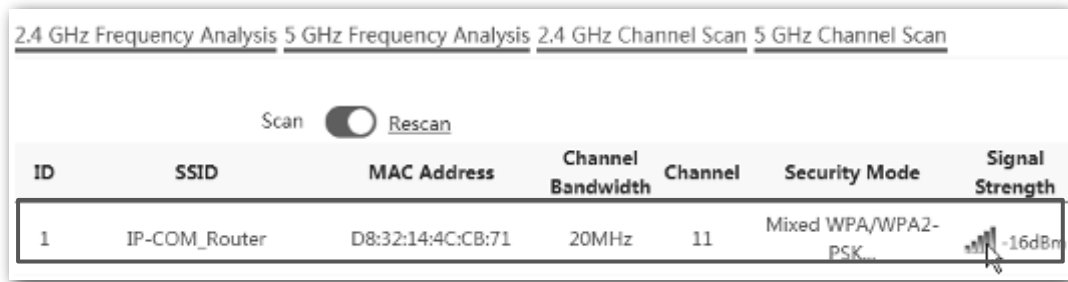
Color-code explanation:

- Red: High channel usage. The channel is not recommended to use.
- Yellow: Moderate channel usage.
- Green: Low channel usage. The channel is recommended to use.

### 5.4.2 Executing channel scan

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

following figure.



## 5.5 WMM

### 5.5.1 Overview

WMM is a wireless QoS protocol used to ensure that packets with high priorities are transmitted first. This ensures better experience of voice and video service over WiFi 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 or longer than a specified period, 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.

#### ■ 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 are not sent again if this policy is adopted. This leads 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.

#### ■ EDCA Parameters

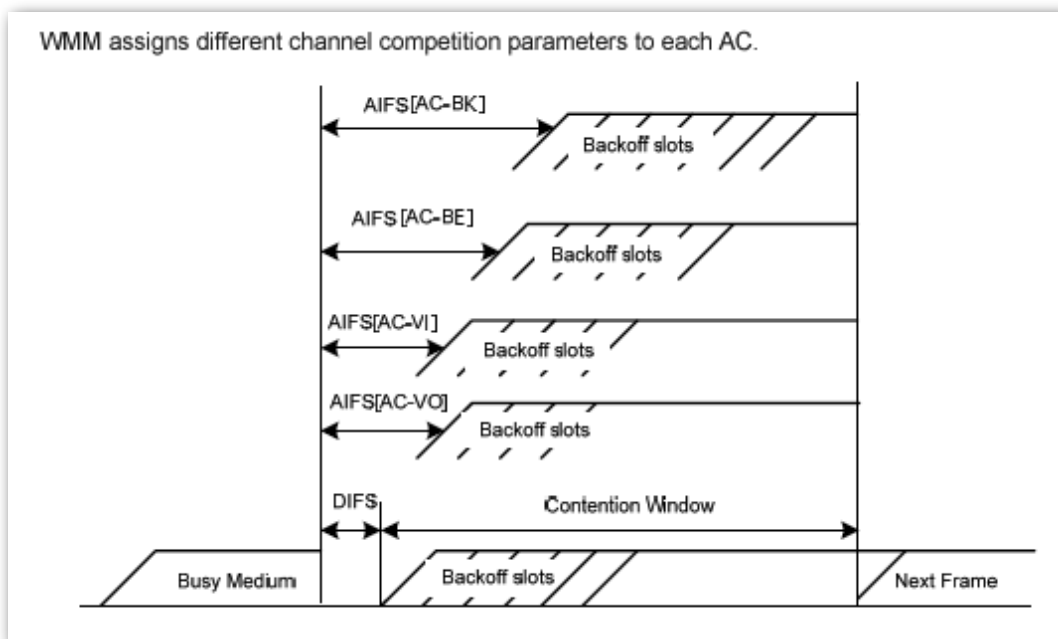
802.11 networks offer wireless access services based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) channel competition mechanism, which allows all wireless devices to fairly compete for channels. All the services implemented over WiFi networks share the same channel competition 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 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 (CWmin) and contention window maximum (CWmax) 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.

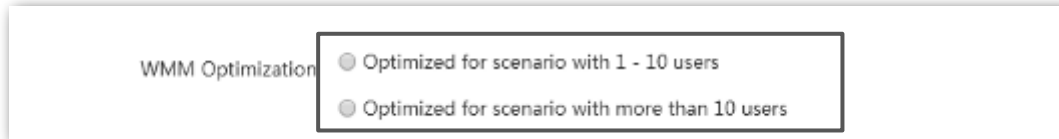


The AP offers **3** options for WMM optimization. You can choose the scenario-based (1 – 10 users, or over 10 users) option and let the AP help you optimize WMM automatically. Or you can choose **Custom** to configure the parameters yourself to meet your very specific requirement.

## 5.5.2 Configuring scenario-based WMM settings

Select either of the two and let the AP help you optimize WMM automatically.

To enter the configuration page, choose **Wireless > WMM**.



The image shows a configuration interface for WMM Optimization. It features a label 'WMM Optimization' on the left. To its right is a rectangular box containing two radio button options. The first option is 'Optimized for scenario with 1 - 10 users' and the second is 'Optimized for scenario with more than 10 users'. Both radio buttons are currently unselected.

According to your actual situations, select **Optimized for scenario with 1 - 10 users** or **Optimized for scenario with more than 10 users**, and click **Save** to apply your settings.

### 5.5.3 Configuring WMM settings manually

Configure the parameters yourself to meet your very specific requirement.

Tick **Custom**, the following page appears. Customize the related parameters and click **Save** to apply your settings.

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="3008"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="1"/>	<input type="text" value="1504"/>

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="3008"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="1504"/>

Save

Cancel

#### Parameter description

Parameter	Description
No ACK	See <a href="#">ACK Policies</a> .
EDCA AP Parameter	See <a href="#">EDCA Parameters</a> .
EDCA STA Parameter	See <a href="#">EDCA Parameters</a> .

## 5.6 Access control

This module allows you to configure MAC address-based wireless access control rules.

### 5.6.1 Overview

To enter the configuration page, choose **Wireless > Access Control**. By default, this function is disabled.

2.4 GHz 5 GHz

SSID: Test\_01

Access Control: ☐

Mode: ☒ Blacklist ☐ Whitelist

MAC Address: Format: XX:XX:XX:XX:XX:XX Add Add Online Devices

ID	MAC Address	Status	Operation
No data			

#### Parameter description

Parameter	Description
SSID	It specifies the SSID on which the MAC address access control is implemented.
Access Control	It specifies whether or not to enable this function.
Mode	<ul style="list-style-type: none"><li>- <b>Blacklist:</b> Clients with MAC addresses on the access control list <b>cannot</b> access the wireless network of AP.</li><li>- <b>Whitelist:</b> Client with MAC addresses on the access control list <b>can</b> access the wireless network of AP.</li></ul>

## 5.6.2 Configuring access control

To enter the configuration page, choose **Wireless > Access Control** first.



- Before configuration, obtain and note down the MAC address(es) of the target device(s).
- The following introduces how to configure on 2.4 GHz band. Configuration on 5 GHz is identical.

### Procedure

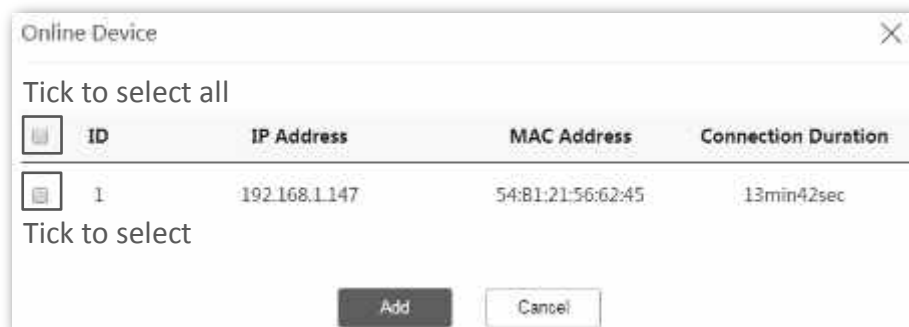
1. Select the SSID to which the access control is applied from the **SSID** drop-down list menu.
2. Enable **Access Control**.
3. Select the control **Mode** as required.
4. Add the MAC address of the client.

#### Option 1: Enter the MAC address manually

Enter the MAC address into the **MAC Address** box.

#### Option 2: Add online clients

- (1) Click **Add Online Devices**. The **Online Device** configuration window appears.



- (2) Select one or multiple devices by ticking the checkbox(es) next to **ID** column.
- (3) Click **Add**.
5. Click **Save** to apply your settings.



SSID

Test\_01

Access Control

Mode

Blacklist

Whitelist

Toggle the button to enable or disable the rule.

MAC Address

Format: XX:XX:XX:XX:XX:XX

Add

Add Online Devices

ID	MAC Address	Status	Operation
1	54:B1:21:56:62:45	<div><div></div>Enable</div>	<div></div>

Save

Cancel

Click to delete the rule.

---End

## 5.7 Advanced settings

This module enables you to make AP's WiFi network and wireless transmission more efficiently through enabling identifying client type and filtering broadcast packet. By default, these two functions are disabled.

To enter the configuration page, choose **Wireless > Advanced Settings**.

### 5.7.1 Identify client type



Note

Enabling this function may impact on the wireless performance of the AP. Therefore, enable this function only when necessary.

With this function enabled, the AP can identify the operating system of the client connected to it. To enable this function, tick **Enable** next to the **Identify Client Type**, and click **Save**.

Advanced Settings

Identify Client Type ☒ Enable ☐ Disable

Broadcast Packet Filter ☐ Enable ☒ Disable

Filters Excludes DHCP and AR ▼

Save Cancel

You can view the client type information by navigating to **Status > Client List**.



Tip

The AP identifies the client type on two conditions:

- The **Identify Client Type** function is enabled.
- The client connected to the AP has accessed an **http://** website.

Otherwise, -- is displayed.

## 5.7.2 Broadcast packet filter



You are strongly recommended to configure this function only under the professional guidance to prevent degrading the WiFi performance of the AP.

By default, the AP will forward lots of invalid broadcast packets, which may affect normal packets transmission. However, this function can filter broadcast packets and reduce airtime consumption, ensuring bandwidth of normal packets transmission.

The AP supports to filter broadcast packets and allows you to keep DHCP and ARP packets, or ARP packets only.

To enter the configuration page, choose **Wireless > Advanced Settings** first.

### Procedure

1. Tick **Enable** next to the **Broadcast Packet Filter**.
2. Select the broadcast packets you do not want to filter from the drop-down list menu of **Filters**.
3. Click **Save** to apply your settings.



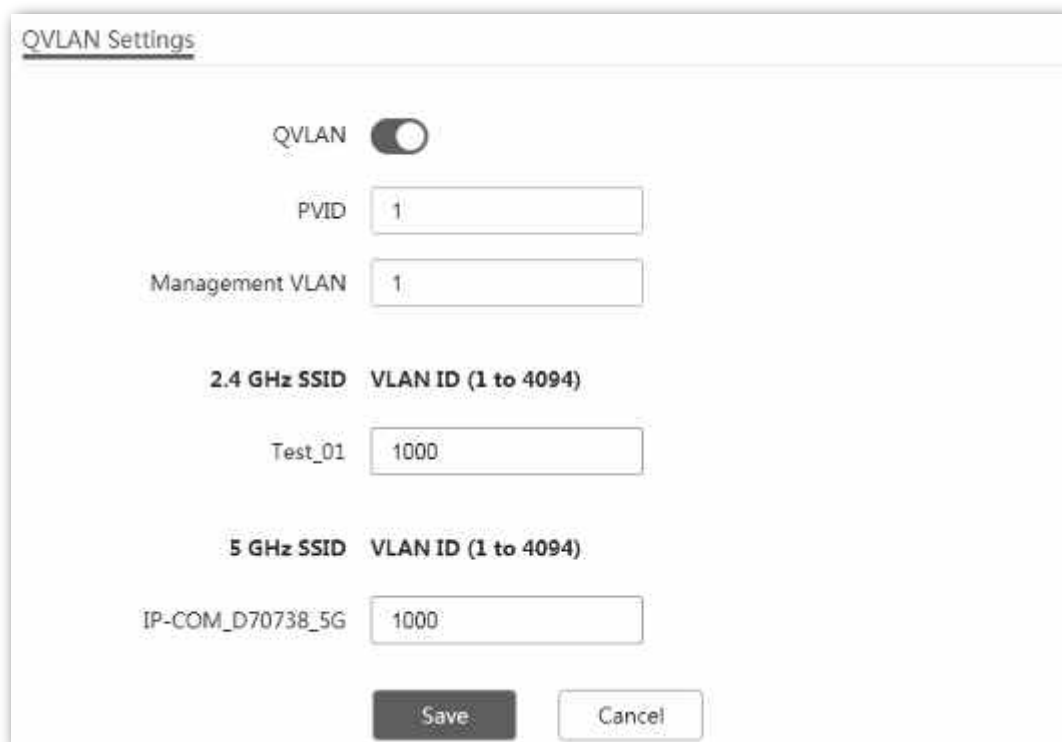
---End

## 5.8 QVLAN settings

This AP supports the IEEE 802.1q VLAN function and can work with switches supporting that function to establish multiple VLANs. Devices connecting to VLANs with different VLAN IDs cannot communicate with each other. By default, the AP's QVLAN function is disabled.

### 5.8.1 Overview

To enter the configuration page, choose **Wireless > QVLAN Settings**.



#### Parameter description

Parameter	Description
QVLAN	It specifies whether to enable the QVLAN function of the AP. By default, it is disabled.
PVID	Port-based VLAN ID. It specifies the ID of the default native VLAN of the trunk port of the AP. The default value is <b>1</b> .
Management VLAN	It specifies the ID of the AP management VLAN. The default value is <b>1</b> . After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.

Parameter	Description
2.4 GHz SSID	It specifies the currently enabled SSID(s) over the 2.4 GHz band of the AP.
5 GHz SSID	It specifies the currently enabled SSID(s) over the 5 GHz band of the AP.
VLAN ID	It specifies the VLAN IDs corresponding to SSIDs. By default, this value is <b>1000</b> . After the QVLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID of an access port is the same as its VLAN ID.

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			Transmit data after removing tags from the data.
Trunk	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.	<p>If the VID and PVID of a port are the same, transmit data after removing tags from the data.</p> <p>If the VID and PVID of a port are different, transmit data without removing tags from the data.</p>

## 5.8.2 Example of configuring QVLAN

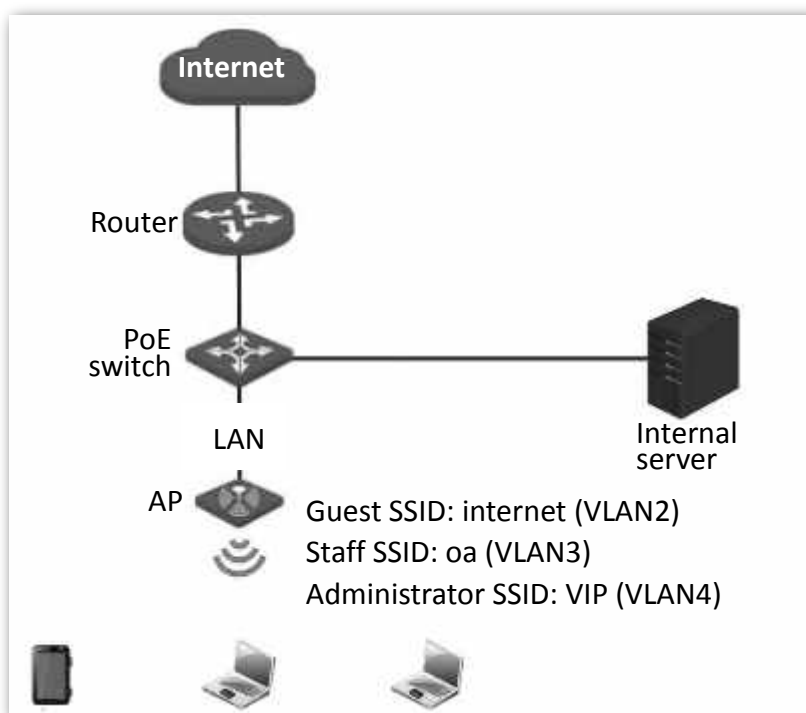
### Networking requirement

A hotel has the following WiFi network coverage requirements:

- Guests are allowed to connect to VLAN2 and only able to access the internet.
- Hotel staffs are allowed to connect to VLAN3 and only able to access the intranet.
- Hotel administrators are allowed to connect to VLAN4, able to access both the intranet and the internet.

Assume that the SSID for guests is **internet**, the SSID for staffs is **oa** and the SSID for administrators is **VIP**. The SSIDs are enabled and configured successfully on the AP.

## Network topology



### Configuration description

Configuring QVLAN function involves operations across various devices. This guide will walk you through the configuration step by step.

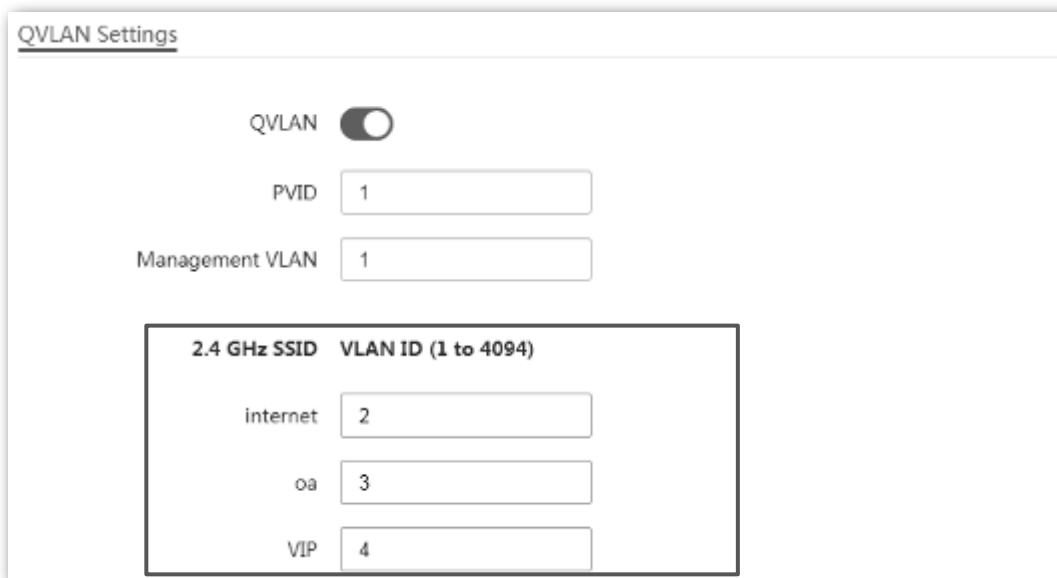
The following table summarizes the overall steps. Get yourself familiar with the whole process before you start.

Step	Task	Description
1	Configure the AP.	Enable QVLAN on the AP, and set required parameters.
2	Configure the switch.	Create IEEE 802.1q VLANs on the switch as required.
3	Configure the router and the internal server.	Enable QVLAN function on your router and internal server, and configure parameters as required.

### Procedure

#### 1. Configure the AP.

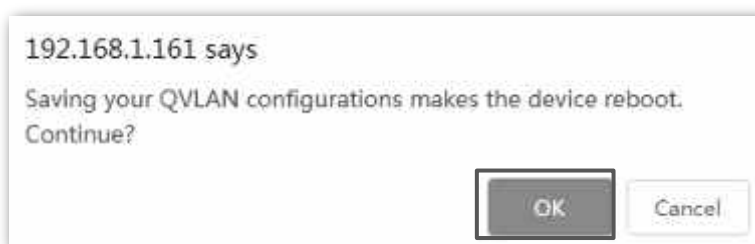
- (1) Log in to the web UI of the AP and choose **Wireless > QVLAN Settings**.
- (2) Enable **QVLAN**.
- (3) Modify the VLAN IDs as shows in the following figure.



The image shows a 'QVLAN Settings' window. At the top, there is a 'QVLAN' toggle switch that is turned on. Below it, there are two input fields: 'PVID' with the value '1' and 'Management VLAN' with the value '1'. A section titled '2.4 GHz SSID' contains a table with two columns: 'SSID' and 'VLAN ID (1 to 4094)'. The table has three rows: 'internet' with VLAN ID '2', 'oa' with VLAN ID '3', and 'VIP' with VLAN ID '4'.

SSID	VLAN ID (1 to 4094)
internet	2
oa	3
VIP	4

- (4) Click **Save** to apply your settings.
- (5) Click **OK**. And wait for the AP completes rebooting.



## 2. Configure the switch.

Create IEEE 802.1q VLANs described in the following table on the switch. Retain the default settings of other ports. For details, refer to the user guide of the switch.

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

## 3. Configure the router and the internal server.

To ensure your wireless devices connected to the AP can access the internet, you should configure QVLAN function on your router and internal server which support QVLAN function. Detailed VLAN parameters are listed as follows:

VLAN parameters configured on your router:

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

VLAN parameters configured on your internal server:

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

For configuration details, refer to the user guides of your router and internal server.

---End

## Verification

Wireless devices connected to the SSID **internet** can access only the internet. Wireless devices connected to the SSID **oa** can access only the intranet. Wireless devices connected to the SSID **VIP** can access both the internet and the intranet.



# 6 Advanced

## 6.1 Deployment mode

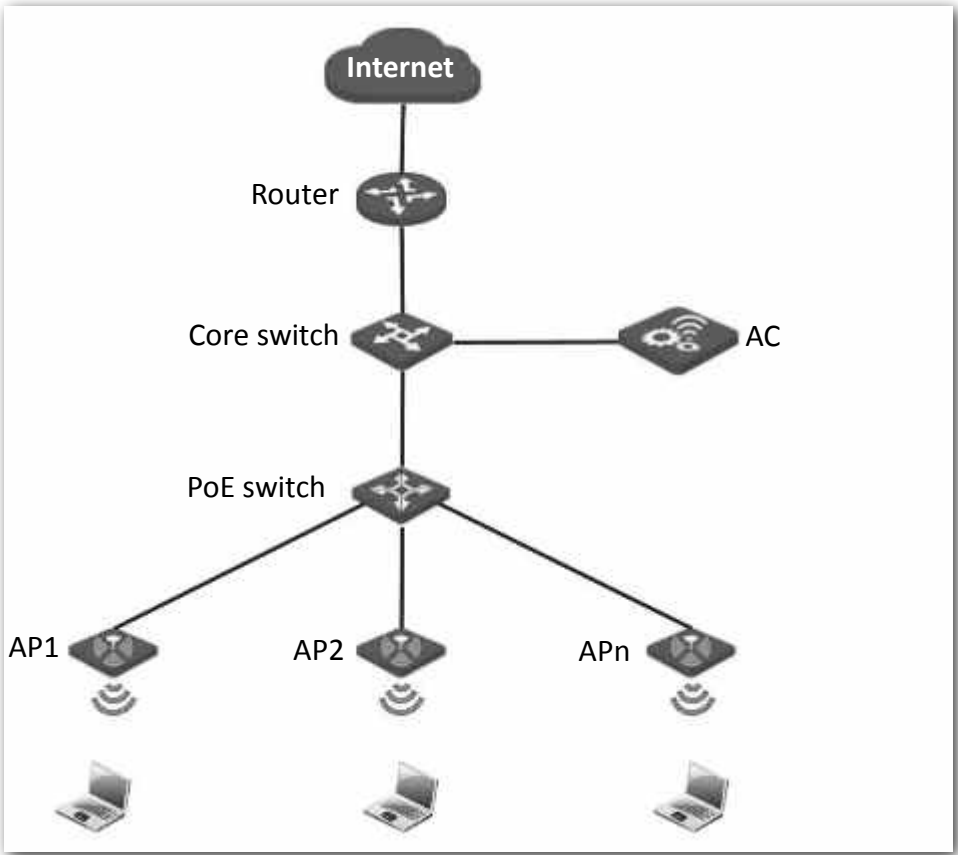
If a large number of APs are deployed, you are recommended to adopt an IP-COM AC (Access Controller, such as AC1000/2000/3000) to manage the APs in a centralized manner. The AP supports **Local Deployment** (default) and **Cloud Deployment**.

### 6.1.1 Applicable scenarios

Deploy your network according to the following introduction to meet your very specific requirement.

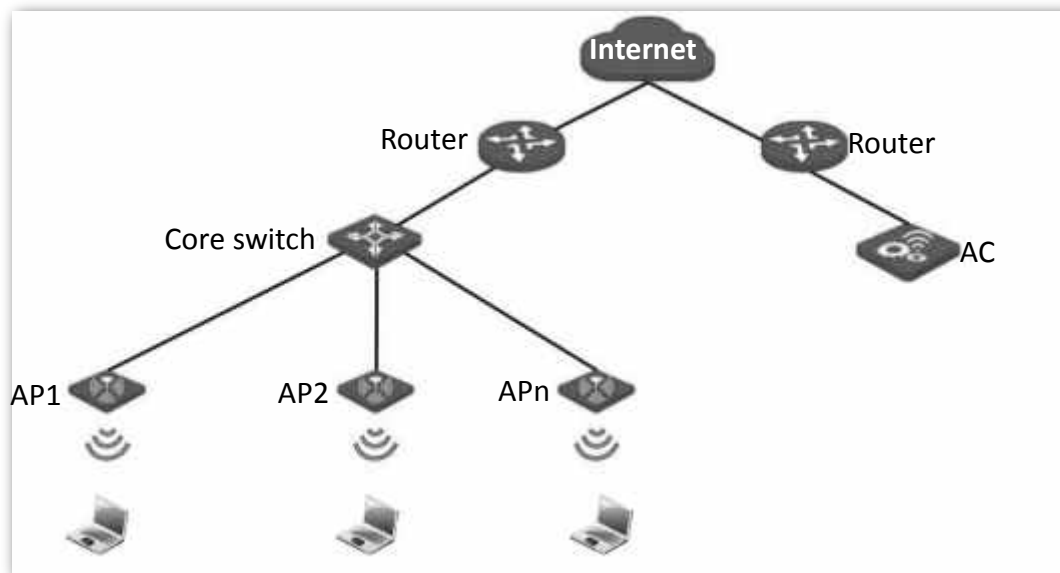
- **Local deployment**

If you need to deploy many APs in a small area, you are recommended to set the AP in the local deployment mode, which uses a local AC (in Sub AC mode) to manage the APs in a centralized manner. The following figure shows the topology for the local deployment mode.



### ■ Cloud deployment

If you need to deploy many APs distributed across a large area, you are recommended to select the cloud deployment mode, which uses an AC (in Cloud AC mode) over the internet to manage the APs in a centralized manner. The following figure shows the topology for the cloud deployment mode.



## 6.1.2 Introduction to deployment mode of the AP

To enter the configuration page, choose **Advanced** > **Deployment Mode**.

Deployment Mode

Deployment Mode: ☒ Local ☐ Cloud


Device Name:

Cloud AC Address:

Cloud AC Management Port:  (Range: 1024 to 65535)

Cloud AC Upgrade Port:  (Range: 1024 to 65535)

### Parameter description

Parameter	Description
Deployment Mode	<p>It specifies the deployment mode supported by the AP.</p> <ul style="list-style-type: none"><li>– <b>Local</b> (default): It indicates that the AP can be managed only through the AC connected to the same local network.</li><li>– <b>Cloud</b>: In this mode, the AP can be managed only by a cloud AC or a cloud server.</li></ul>
Device Name	<p>It specifies the device name of the AP.</p> <p> Tip</p> <ul style="list-style-type: none"><li>– You can customize the device name here, or on <b>Internet Settings &gt; LAN Setup</b> page. Modification of the device name is globally applied.</li><li>– For later convenient management, you are recommended to customize the device name.</li></ul>
Cloud AC Address	<p>It specifies the WAN IP address of the router to which the cloud AC connects, or the domain name to which the router's WAN IP address is bound.</p>
Cloud AC Management Port	<p>It specifies port of the egress router to which the cloud AC connects for managing this device.</p>
Cloud AC Upgrade Port	<p>It specifies port of the egress router to which the cloud AC connects for upgrading this device.</p>

## 6.1.3 Configuring the cloud deployment mode

### Procedure

1. Click **Deployment**, and select **Cloud**.
2. Set related parameters.
3. Click **Save** to apply your settings.

Deployment

Administrator: admin

Deployment

☐ Local

☒ Cloud

Device Name

Access Point

Cloud AC Management Port

(Range: 1024 to 65535)

Cloud AC Upgrade Port

(Range: 1024 to 65535)

Cloud AC Address

(IP address or domain name of WAN port of the egress router which the remote AC connects)

Save

Restore

Help

---End

## 6.2 SNMP

### 6.2.1 Overview

The Simple Network Management Protocol (SNMP) is the most widely used network management protocol in TCP/IP networks. SNMP enables you to remotely manage all your network devices compliant with this protocol, such as monitoring the network status, changing network device settings, and receiving network event alarms.

SNMP supports managing devices bought from various vendors automatically, regardless of physical differences among the devices.

#### SNMP management framework

The SNMP management framework consists of SNMP manager, SNMP agent, and Management Information Base (MIB).

- **SNMP manager:** It is a system that controls and monitors network nodes using the SNMP protocol. Network Management System (NMS) is the most widely used SNMP manager in network environments. An NMS can be a dedicated network management server, or an application that implements management functions in a network device.
- **SNMP agent:** It is a software module in a managed device. This module is used to manage data about the device and report the management data to an SNMP manager.
- **MIB:** It is a collection of managed objects, defining a series of attributes of managed objects, including names, access permissions, and data types of objects. Each SNMP agent has its own MIB. An SNMP manager can read and/or write objects in the MIB based on the permissions assigned to the SNMP manager.

An SNMP manager manages SNMP agents in an SNMP network. The SNMP manager exchanges management information with the SNMP agents using the SNMP protocol.

#### Basic SNMP operations

The AP supports the following basic SNMP operations:

- **Get:** An SNMP manager performs this operation to query the SNMP agent of the AP for values of one or more objects.
- **Set:** An SNMP manager performs this operation to set values of one or more objects in the MIB of the SNMP agent of the AP.

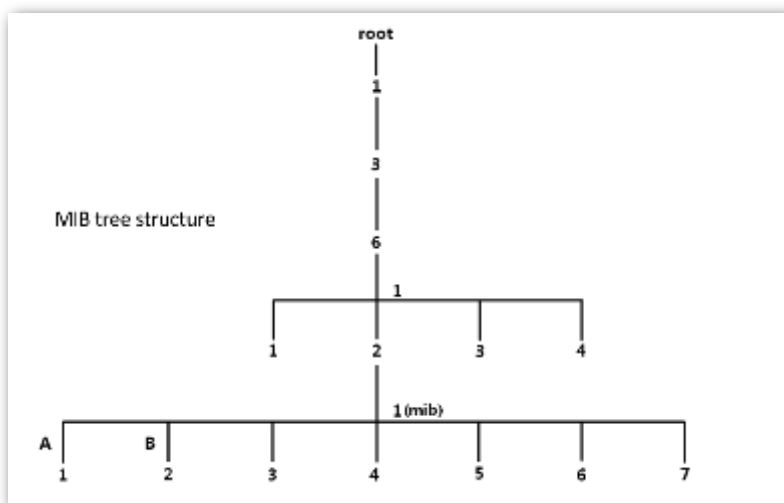
## SNMP protocol version

The AP is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism. Community name is used to define the relationship between an SNMP agent and an SNMP manager. If the community name contained in an SNMP packet is rejected by a device, the packet is discarded. A community name functions as a password to control SNMP agent access attempts of SNMP managers.

SNMP V2C is compatible with SNMP V1 and provides more functions than SNMP V1. Compared with SNMP V1, SNMP V2C supports more operations (GetBulk and InformRequest) and data types (such as Counter64), and provides more error codes for better distinguishing errors.

## MIB introduction

An MIB adopts a tree structure. The nodes of the tree indicate managed objects. A path consisting of digits and starting from the root can be used to uniquely identify a node. This path is called an object identifier (OID). The following figure shows the structure of an MIB. In the figure, the OID of A is 1.3.6.1.2.1.1, whereas the OID of B is 1.3.6.1.2.1.2.

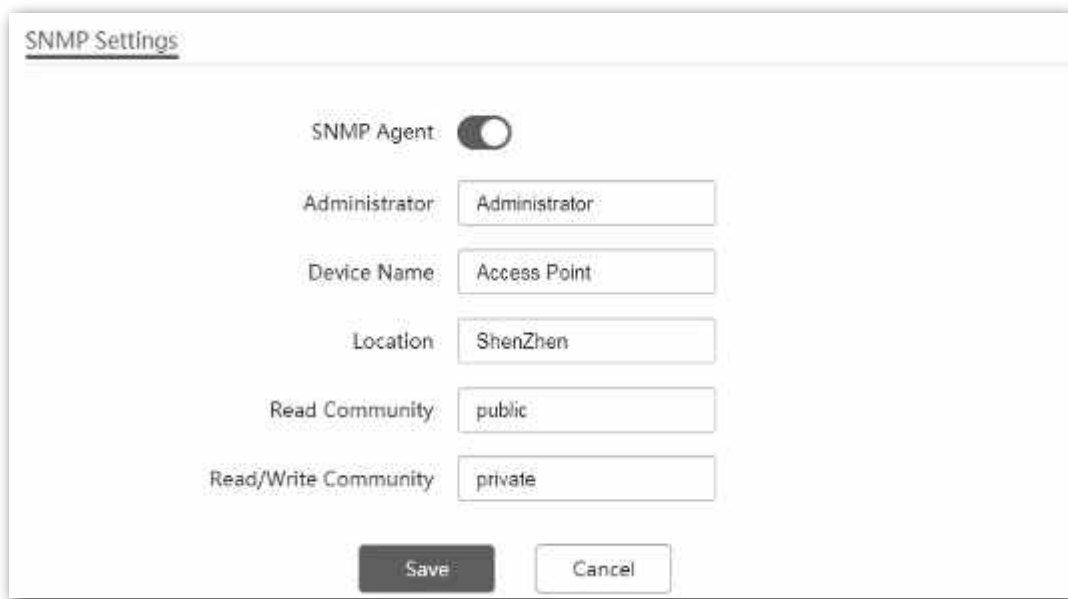


## 6.2.2 Configuring the SNMP function

To enter the configuration page, choose **Advanced > SNMP** first.

### Procedure


1. Enable **SNMP Agent**.
2. Set related parameters.
3. Click **Save** to apply your settings.



The image shows a 'SNMP Settings' configuration window. It contains a toggle switch for 'SNMP Agent' which is currently turned off. Below this are several text input fields: 'Administrator' (containing 'Administrator'), 'Device Name' (containing 'Access Point'), 'Location' (containing 'ShenZhen'), 'Read Community' (containing 'public'), and 'Read/Write Community' (containing 'private'). At the bottom of the window are two buttons: 'Save' and 'Cancel'.

---End

### Parameter description

Parameter	Description
SNMP Agent	<p>It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled.</p> <p>An SNMP manager and the SNMP agent can communicate with each other only when their SNMP versions are the same. Currently, the SNMP agent function of the AP supports SNMP V1 and SNMP V2C.</p>
Administrator	<p>It specifies the administrator's name of the AP. The default name is <b>Administrator</b>. You can modify the administrator's name if required.</p>
Device Name	<p>It specifies the device name of the AP. By default, the device name is <b>Access Point</b>. You can modify it if required.</p> <div> Tip</div> <p>You are recommended to modify the AP name so that you can identify your AP</p>

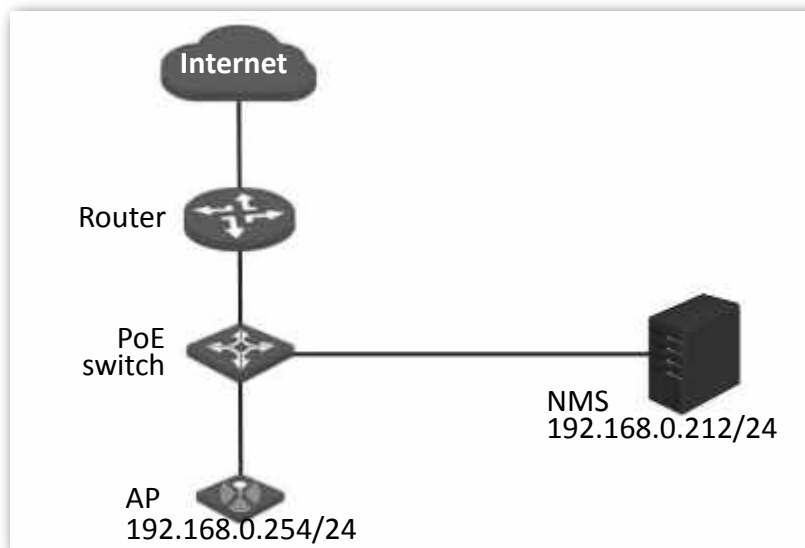


Parameter	Description
	easily when managing the AP using SNMP.
Location	It specifies the location where the AP is used. You can modify the location according to your actual situation.
Read Community	It specifies the read password shared between SNMP managers and the SNMP agent. The default password is <b>public</b> . The SNMP agent function of the AP allows an SNMP manager to use the password to read variables in the MIB of the AP.
Read/Write Community	It specifies the read/write password shared between SNMP managers and the SNMP agent. The default password is <b>private</b> . The SNMP agent function of the AP allows an SNMP manager to use the password to read/write variables in the MIB of the AP.

### 6.2.3 Example of configuring SNMP settings

#### Networking requirement

- The AP connects to an NMS over an LAN network. This IP address of the AP is 192.168.0.254/24 and the IP address of the NMS is 192.168.0.212/24.
- The NMS uses SNMP V1 or SNMP V2C to monitor and manage the AP.



#### Procedure

##### 1. Configure the AP.

Assume that the administrator name is **Tom**, read community is **Tom**, and read/write community is **Tom123**.

- (1) Log in to the web UI of the AP and choose **SNMP**.

- (2) Set **SNMP Agent** to **Enable**.
- (3) Set the SNMP parameters.
- (4) Click **Save** to apply your settings.



The image shows a configuration dialog box for the SNMP Agent. It contains the following fields and controls:

- SNMP Agent:** A toggle switch that is currently turned on (indicated by a dark circle).
- Administrator:** A text input field containing the value "Tom".
- Device Name:** A text input field containing the value "Access Point".
- Location:** A text input field containing the value "ShenZhen".
- Read Community:** A text input field containing the value "Tom".
- Read/Write Community:** A text input field containing the value "Tom123".
- Buttons:** At the bottom, there are two buttons: "Save" (dark grey) and "Cancel" (light grey).

## 2. Configure the NMS.

On an NMS that uses SNMP V1 or SNMP V2C, set the read community to **Tom** and read/write community to **Tom123**. For details about how to configure the NMS, refer to the user guide of the NMS.

---End

### Verification

After the configuration, the NMS can connect to the SNMP agent of the AP and can query and set some parameters on the SNMP agent through the MIB.

# 7 Tools

## 7.1 Date & time

This section introduces how to set the system time and login timeout interval of your AP.

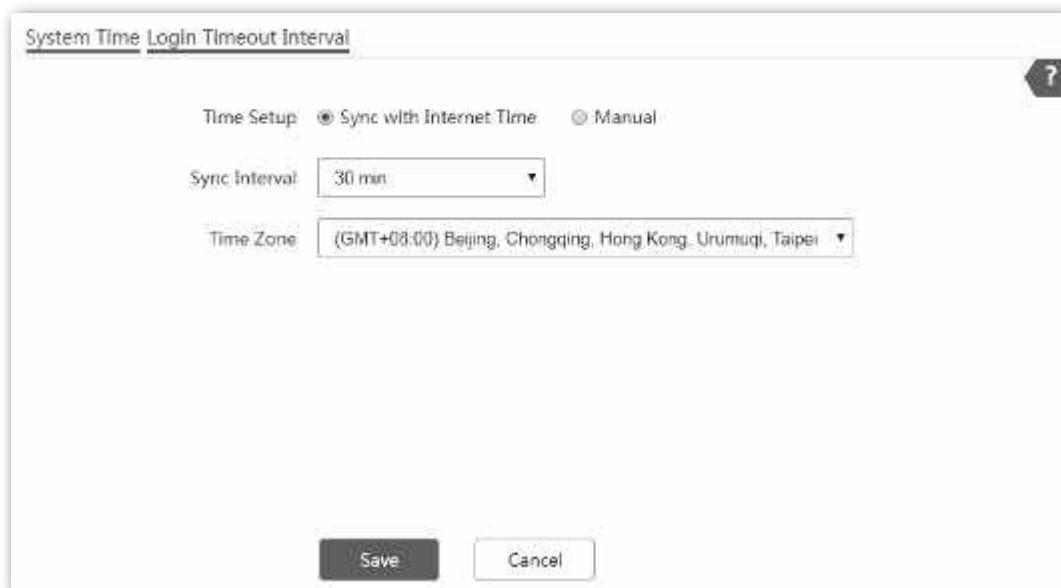
### 7.1.1 Overview

This function is used to set the system time. To make the time-related functions effective, ensure that the system time of the AP is set correctly.

The section introduces how to:

- Sync with internet time.
- Set system time manually (default).

To access the configuration page, choose **Tools > Date & Time**. See the following figure.



The screenshot shows a configuration window titled "System Time" with a sub-tab "Login Timeout Interval". The window contains the following elements:

- Time Setup:** Two radio buttons. "Sync with Internet Time" is selected (indicated by a filled circle), and "Manual" is unselected (indicated by an empty circle).
- Sync Interval:** A dropdown menu currently showing "30 min".
- Time Zone:** A dropdown menu showing "(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei".
- Buttons:** "Save" and "Cancel" buttons at the bottom.
- Help:** A question mark icon in the top right corner.

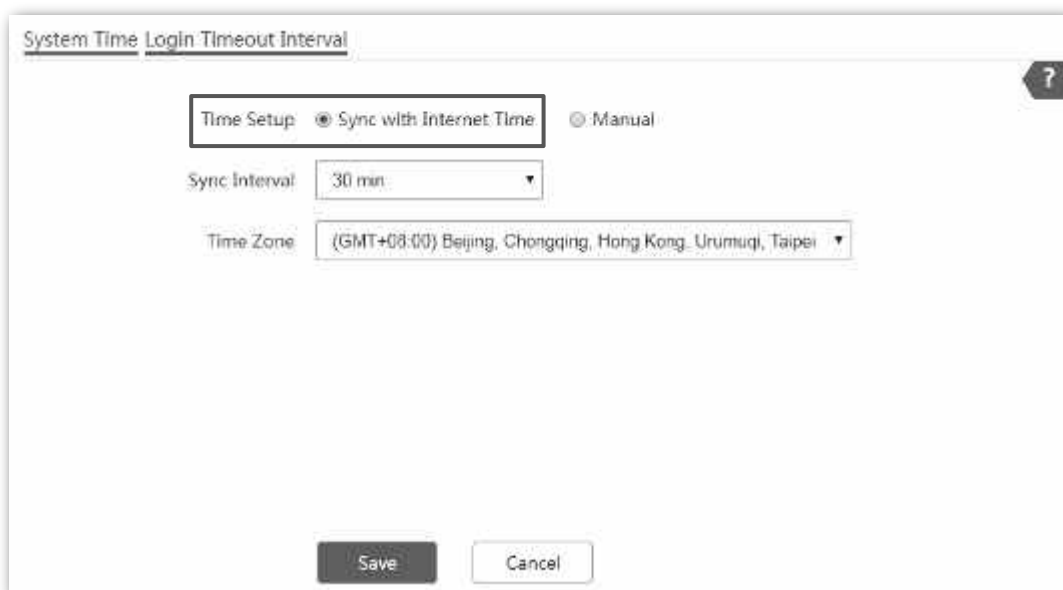
## 7.1.2 Configuring system time

### Configuring AP to synchronizing with internet time

With this method, the AP automatically synchronizes its system time with the network time server (NTS). As long as the AP is connecting to the internet, the system time is correct.

#### Procedure

1. Choose **Tools > Date & Time**.
2. Tick the **Sync with Internet Time** box.
3. Select a value from the **Sync Interval** drop-down list menu as required, which is **30 min** in this example.
4. Choose the **Time Zone** where the AP locates.
5. Click **Save** to apply your settings.



The screenshot shows a web-based configuration window titled "System Time Login Timeout Interval". It has two tabs: "System Time" (active) and "Login Timeout Interval". In the "System Time" tab, there are two radio buttons under "Time Setup": "Sync with Internet Time" (selected) and "Manual". Below this, there is a "Sync Interval" dropdown menu set to "30 min" and a "Time Zone" dropdown menu set to "(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei". At the bottom of the window are "Save" and "Cancel" buttons.

---End

The AP synchronizes with the internet time every 30 minutes.

### Configuring date and time manually

With this method, you need to manually reconfigure the system time each time the AP reboots.

### Procedure

1. Choose **Tools > Date & Time**.
2. For manual setup, you can:

**Option one:** Enter a correct date and time manually.

**Option two:** Click **Sync with PC Time**, the AP auto-fills the system time of your management computer in the **Date & Time** fields.



Tip

Make sure that the system time of your management computer is correct.

---

3. Click **Save** to apply your settings.

---End

## 7.1.3 Configuring 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 automatically.

### Procedure

1. Choose **Tools > Date & Time**, and click the **Login Timeout Interval** tab.
2. Set the login timeout interval as required.

3. Click **Save** to apply your settings.



The screenshot shows a configuration window titled 'System Time Login Timeout Interval'. The window has a tabbed interface with 'System Time' and 'Login Timeout Interval'. The 'Login Timeout Interval' tab is active. Inside the tab, there is a label 'Login Timeout Interval' followed by a text input field containing the value '5'. To the right of the input field is a hint text: 'min(Range: 1 to 60, Default: 5)'. At the bottom of the window, there are two buttons: 'Save' and 'Cancel'. A help icon (?) is located in the top right corner of the window.

---End

The AP logs you out automatically if you perform no operation within the interval you set here.

## 7.2 Maintenance

This section introduces how to:

- Reboot the AP manually, or as scheduled.
- Reset the AP either using web UI, or the RESET button.
- Upgrade the AP.
- Back up the AP's configuration to your local computer.
- Restore your previous configurations.
- Control the LED indicator of the AP.

### 7.2.1 Reboot

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

The AP supports two rebooting methods:

- **Manual reboot:** Reboot the AP by clicking the Reboot button.
- **Reboot schedule:** Let the AP reboot at the specified time or interval you set.



Note

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

---

### Manual reboot

#### Procedure

1. Choose **Tools > Maintenance**.
2. Click **Reboot**.
3. Click **OK** on the pop-up window.



---End

Wait for the AP completes rebooting.

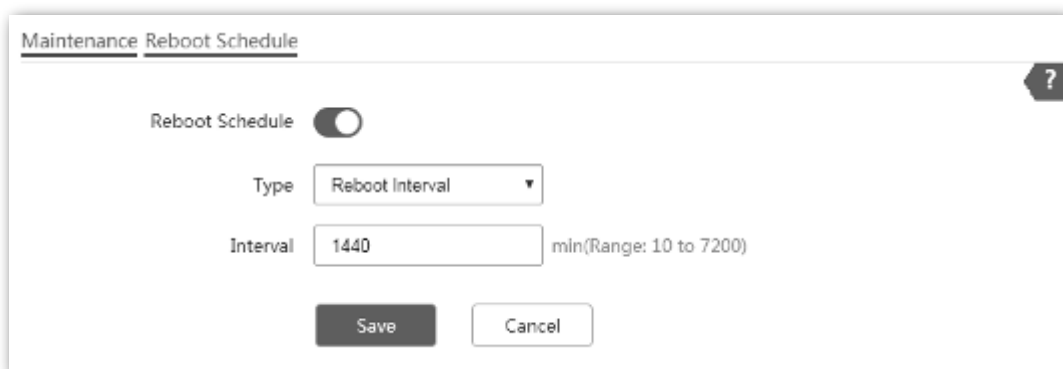
## Reboot schedule

You can let the AP reboot:

- **At interval:** The AP reboots at the interval you set.
- **At specified time:** The AP reboots regularly at the time you set.

### ■ Configuring the AP to reboot at an interval

1. Click **Tools > 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.



The screenshot shows a web interface for configuring the Reboot Schedule. At the top, there are two tabs: 'Maintenance' and 'Reboot Schedule', with 'Reboot Schedule' being the active tab. Below the tabs, there is a toggle switch for 'Reboot Schedule' which is currently turned on. Underneath the toggle, there is a 'Type' dropdown menu set to 'Reboot Interval'. Below that, there is an 'Interval' input field containing the value '1440', with a note 'min(Range: 10 to 7200)' to its right. At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

---End

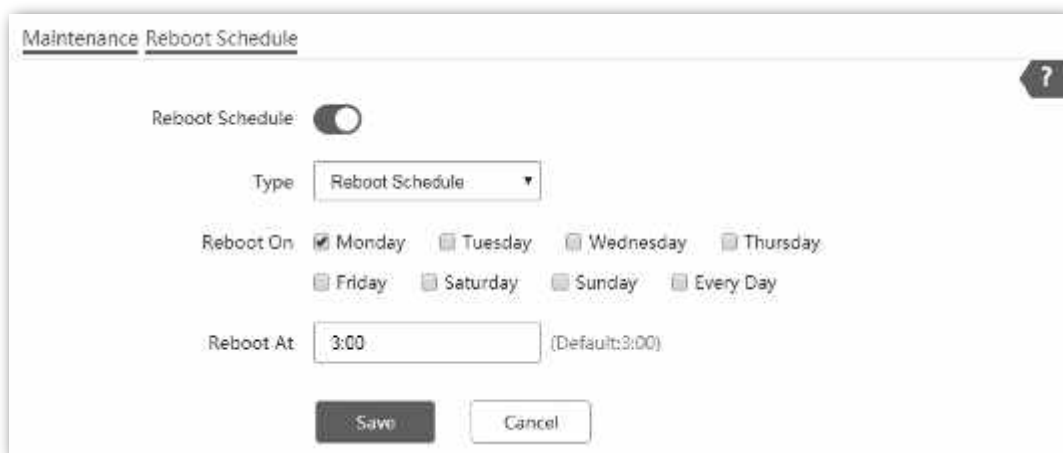
The AP reboots every 1440 minutes.

### ■ Configuring the AP to reboot at specified time

1. Click **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.



The screenshot shows a web interface window titled "Maintenance Reboot Schedule". It features a "Reboot Schedule" toggle switch that is turned on. Below the toggle is a "Type" dropdown menu set to "Reboot Schedule". Under "Reboot On", there are checkboxes for days of the week: Monday (checked), Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday, along with an "Every Day" option. The "Reboot At" field is set to "3:00" with a "(Default:3:00)" note. At the bottom are "Save" and "Cancel" buttons.

---End

The AP reboots at 3:00 every Monday.

## 7.2.2 Reset

If the internet is inaccessible for unknown reasons, or you forget the login password, you can reset the AP to resolve the problems.

The AP supports two resetting methods:

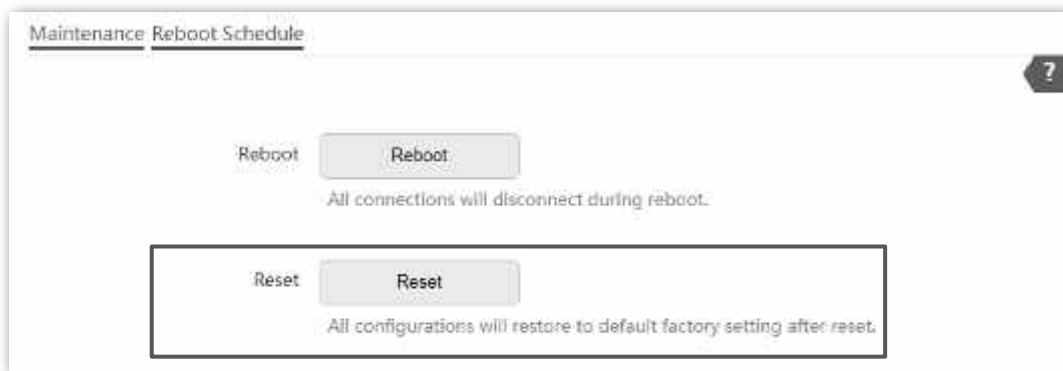
- [Resetting the AP using web UI.](#)
- [Resetting the AP using the Reset button.](#)



- Resetting the AP deletes all your current configurations, and you need to reconfigure the AP again. Therefore, resetting the AP only when necessary.
  - If it is necessary to reset the AP, backing up your current configuration first.
  - When resetting, do not power off the AP.
- 

### Resetting the AP using web UI

1. Click **Tools > Maintenance**.
2. Click the **Reset** button.
3. Click **OK** on the pop-up window.



---End

## Resetting the AP using the Reset button

This method enables you to reset the AP without logging in to its web UI.

With the SYS LED indicator blinking, hold down the **RESET** button using a paper clip for about 8 seconds, and release the button when the SYS LED indicator lights up. Wait until the AP completes resetting.

---End

## 7.2.3 Upgrade firmware

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



Note

- 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 <http://www.ip-com.com.cn> to your local computer.
2. Log in to the web UI of the AP, navigate to **Tools > Maintenance**, and locate the **Upgrade Firmware** configuration area.
3. Click **Upgrade**, select and upload the firmware that has been downloaded to your computer.

4. Click **Upgrade**. Wait until the progress bar completes.



Note

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

---

---End

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

## 7.2.4 Backup and restoring configurations

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.

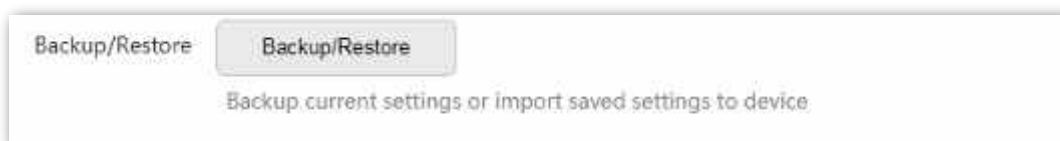


If you need to apply same or similar configuration to many APs, you can configure one of the APs, back up its configuration, and use the backup configuration file to restore the configuration of other APs.

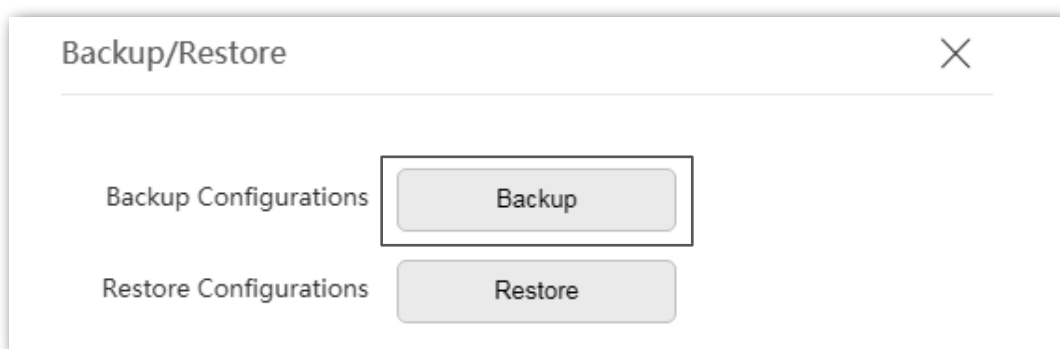
---

### Backup the current configuration

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



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

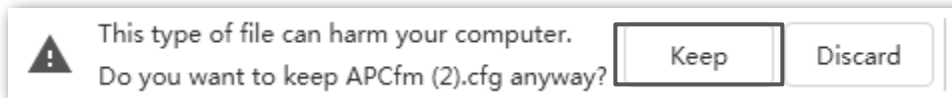


---End

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

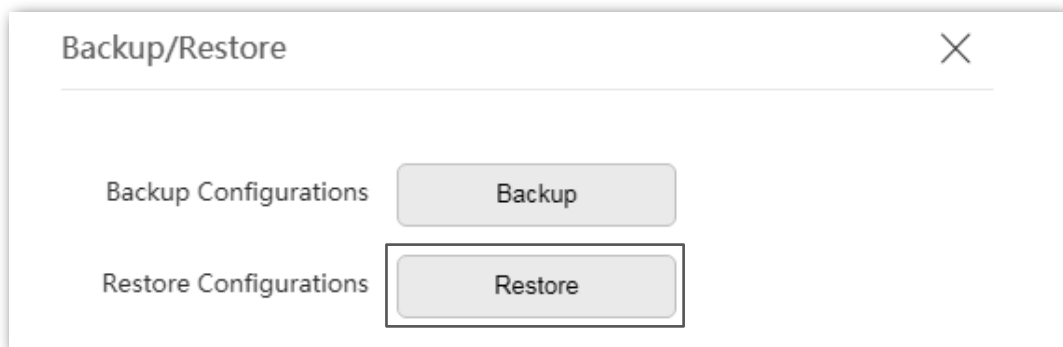


If the following warning message appears, click **Keep**.



## Restoring previous configuration

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



4. Choose the file you would like to restore.

---End

Wait until the progress bar completes.

## 7.2.5 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. To turn off the LED indicator, click **Turn off all LED indicators**.



## 7.3 Account

### 7.3.1 Overview

The router supports two account types: **Administrator** and **Guest**. The difference between them is their permission.

The **Administrator** account has permission to view and modify the settings. The default username and password for this account are **admin/admin** (both are case-sensitive). You can view and modify it here.

The **Guest** account can only view other than modifying the settings. The default username and password for this account are **user/user** (both are case-sensitive). You can view and modify it here.

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



### 7.3.2 Modifying login password

1. Click **Tools > Account** to enter the configuration page.
2. Locate the account type and modify the password on the pop-up window.
3. Click **Save** to apply your settings.

---End

Then you will be redirected to the login page. Enter the password corresponding to the account you set just now, and click **Login** to log in to the AP.

## 7.4 System Log

System logs record information about system running status and the operation you performed on it. When system malfunctions occur, you can use system log for troubleshooting.

The AP also supports **Log Service** that allows you to sync the system logs of the AP to the log server you specified. Therefore, you can use syslog software to view the logs on the server.

### 7.4.1 Viewing system logs



Tip

- System logs will be cleared each time the AP reboots or resets.
- By default, the system only keeps 150 logs that are generated the most recently.

To view system logs, choose **Tools > System Log**.

Click **Refresh** to refresh the current page.

Click **Clear** to clear all logs.

Logs Log Settings

Refresh

Clear

Log Type: All

ID	Time	Type	Log Content
1	2019-03-30 13:34:38	System	web 192.168.1.182 login
2	2019-03-30 13:34:38	System	web login time expired
3	2019-03-30 13:34:31	System	web login time expired
4	2019-03-30 12:26:07	System	AP enter in receive scan status.
5	2019-03-30 11:38:33	System	web 192.168.1.182 login
6	2019-03-30 11:37:38	System	web 192.168.1.182 login
7	2019-03-30 11:37:27	System	Login manage: Change user passwo...
8	2019-03-30 11:31:59	System	web 192.168.1.182 login
9	2019-03-30 11:31:37	System	web 192.168.1.182 login
10	2011-05-01 00:00:47	System	web 192.168.1.182 login

10

in total/Page 24 in total

Previous

1

2

3

Next

## 7.4.2 Modifying number of logs to be displayed on Web UI

### Procedure

Choose **System Log**, and then click the **Log Settings** page first.

1. Enable **Log Service**.



The screenshot shows a web interface titled "Logs Log Settings". It contains a "Log Service" toggle switch that is currently turned off. Below the toggle is a "Number of Logs" input field with the value "150" and a range note "(Range: 100 to 300, Default: 150)".

2. Modify the **Number of Logs** as required.
3. Click **Save** at the bottom on this page to apply your settings.

---End

## 7.4.3 Sync system logs of the AP to a log server

With the **Log Service** function enabled, you can sync the system logs of the AP to the log server you specified. Therefore, you can use syslog software to view the AP's system logs on the log server.

### Procedure

1. Choose **Tools > System Log**, and click the **Log Settings** tab.
2. Enable **Log Service**, and click **Save** to apply your settings.



Logs Log Settings

Log Service ☐

Number of Logs  (Range: 100 to 300, Default: 150)

ID	Log Server IP Address	Log Server Port	Status	Operation
No data				

Add

Save Cancel

- Click **Add**. The following window appears.

Log Server IP Address

Log Server Port

Status ☒ Enable ☐ Disable

Add Cancel

- Enter the **Log Server IP Address** and **Log Server Port** as required, which is **192.168.20.213** and **514** in this example. And click **Add**.

Logs

Log Settings

Log Service

☐

Number of Logs

(Range: 100 to 300. Default: 150)

ID	Log Server IP Address	Log Server Port	Status	Operation
1	192.168.20.213	514	Enable	<div><div></div><div></div></div>

Add

Save

Cancel

---End

You can view the system log of the AP remotely on the third-party log server software you use.

## 7.5 Diagnostic tool

### 7.5.1 Overview

The AP supports Ping command, which is used to check whether or not the connection between the AP and a specified host is correct and the connection quality when facing network reachability issues.

### 7.5.2 Executing Ping command to detect connection quality

Assume that you need to check the connection quality between the AP and its upstream router:

1. Choose **Tools > Diagnostic Tool** to enter the configuration page.
2. Enter the IP address of its upstream router in the **Target IP/Domain Name** box, which is **192.168.20.231** in this example.



3. Click **ping**, or press **Enter** (Windows) or **Return** (Mac) on keyboard.  
--- End

Wait a moment. The Ping result is displayed in the black square. See the following figure:

Diagnostic Tool

?

Enter an IP address (eg. 192.168.0.254) or a domain name (eg. www.google.com)

Target IP/Domain Name

```
Ping 192.168.20.231(192.168.20.231):56 data bytes
64 bytes from 192.168.20.231: seq=0 ttl=64 time=0.768 ms
64 bytes from 192.168.20.231: seq=1 ttl=64 time=0.587 ms
64 bytes from 192.168.20.231: seq=2 ttl=64 time=0.587 ms
64 bytes from 192.168.20.231: seq=3 ttl=64 time=0.618 ms

--- 192.168.20.231 ping statistics ---
4 packets transmitted, 4 packets recieved, 0% packet loss
roud-trip min/avg/max = 0.587/0.640/0.768 ms
```

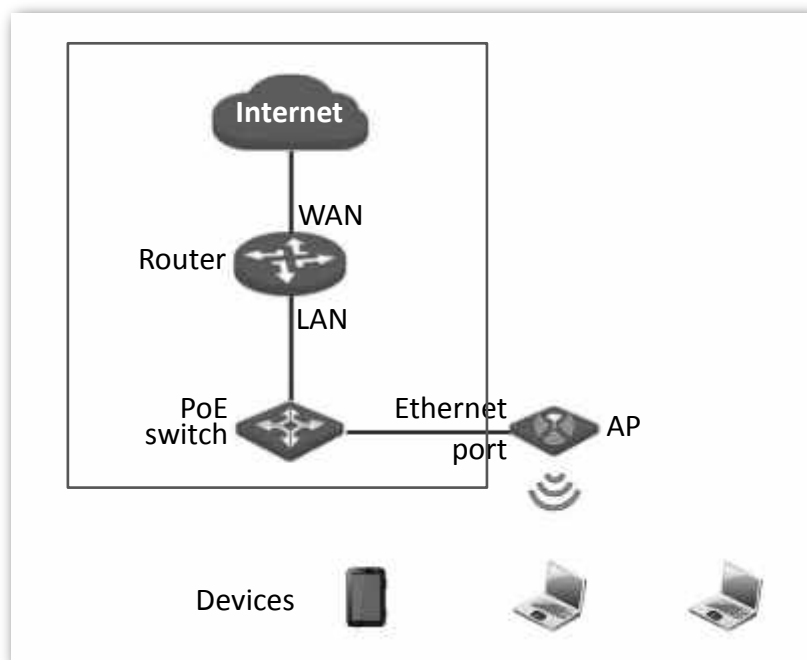
## 7.6 Uplink check

### 7.6.1 Overview

In AP mode, the AP connects to its upstream network using the LAN port. If a critical node between the LAN port and the upstream network fails, the AP as well as the wireless devices connected to the AP cannot access the upstream network. If uplink detection is enabled, the AP regularly pings specified hosts through the LAN port. If all the hosts are not reachable, the AP stops its wireless service and wireless devices cannot find the SSIDs of the AP. The device 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 devices can connect to the upstream network through another nearby AP that works properly.

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



### 7.6.2 Configuring uplink detection

To enter the configuration page, choose **Tools > Uplink Detection** first.

#### Procedure

1. Enable **Uplink Detection**.

2. Enter the LAN IP address of **Host1** and **Host2** to ping in the corresponding box.



Tip

Both **Host1 to Ping** and **Host2 to Ping** are mandatory. If you have only one host to ping, repeat the IP address of Host1 in **Host2 to Ping** box.

---

3. Enter the interval at which the AP detects its uplink in **Ping Interval** box.
4. Click **Save** to apply your settings.

Uplink Detection

Uplink Detection ☐

Host1 to Ping 192.168.1.161

Host2 to Ping 192.168.1.1

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


Save Cancel

---End

# Appendix

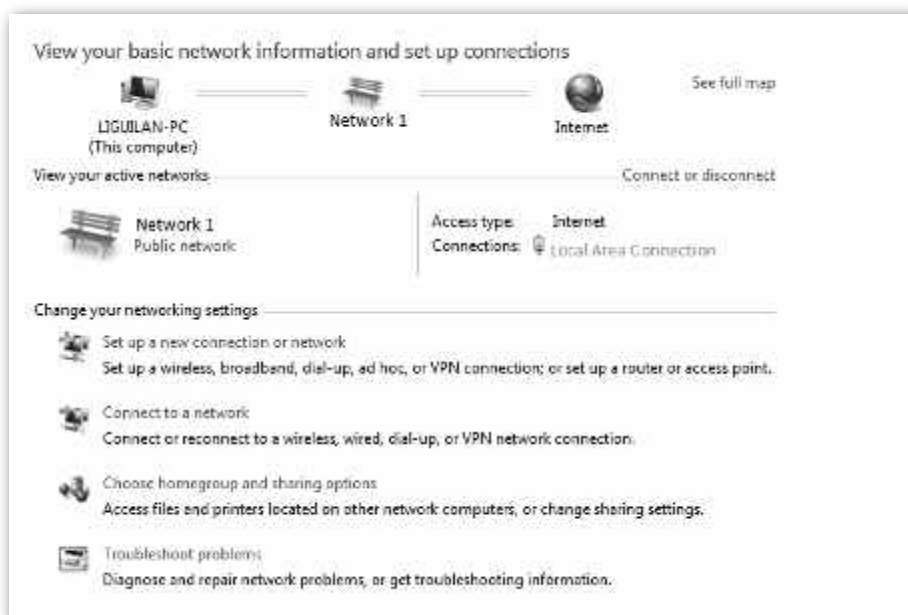
## A.1 Configuring a static IP address for your computer (Example: Windows 7)

### Procedure

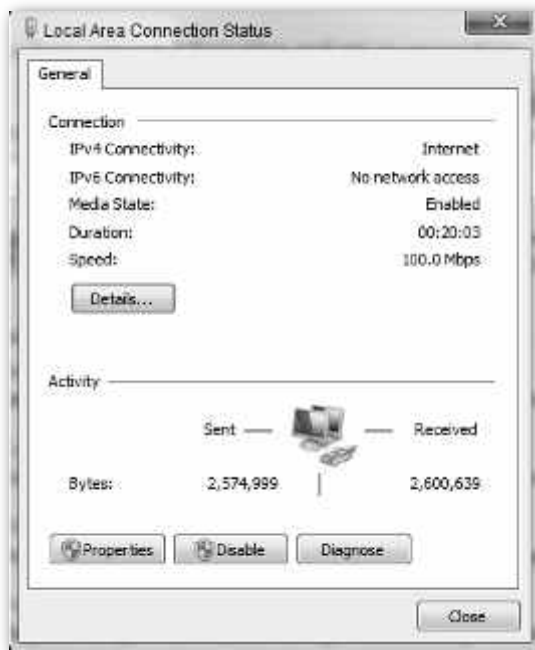
1. Right-click  in the lower-right corner of the desktop and choose **Open Network and Sharing Center**.

Open Network and Sharing Center

2. Click **Local Area Connection**.



3. Click **Properties**.



4. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.





5. Select **Use the following IP address** and **Use the following DNS server address**.




6. **IP address, Subnet mask:** Set a static IP address, subnet mask for your computer, which is **192.168.0.10** and **255.255.255.0** in this example, and click **OK**.



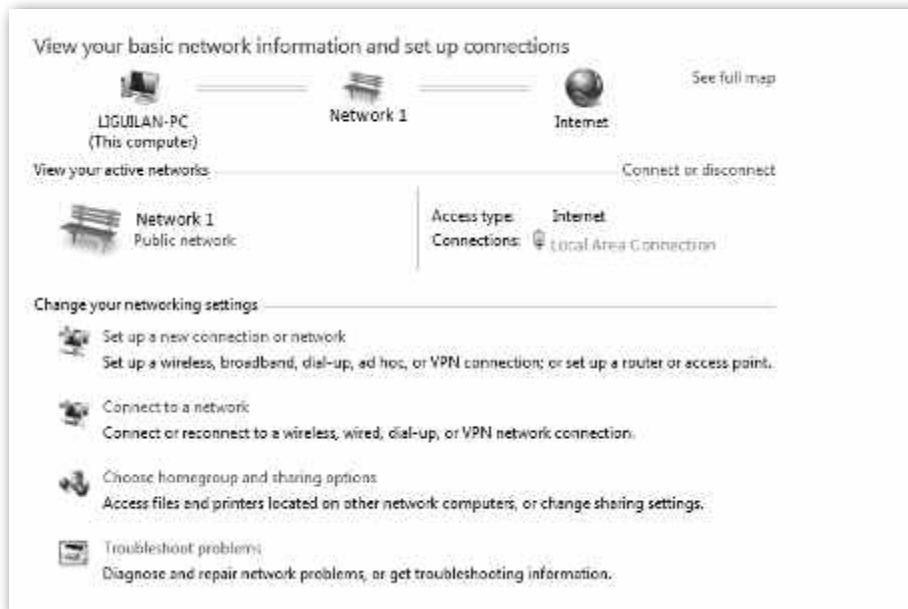
## Verification

Configuration succeeds. You can check whether your configuration is successful on the **Network Connection Details** page. Procedure are as follows:

1. Right-click  in the lower-right corner of the desktop and choose **Open Network and Sharing Center**.

Open Network and Sharing Center

2. Click **Local Area Connection**.



3. Click **Details**.



4. Check whether your configuration is successful on the **Network Connection Details** page. Parameters in **IPv4 Address**, **IPv4 Subnet Mask** represent the IP address, subnet mask of your computer.



## A.2 FAQ

**Q1: I cannot access the web UI of the AP after entering 192.168.0.254. What should I do?**

**A1:** Try the following solutions:

- Ensure that all your Ethernet cables are properly connected.
- If there is no IP-COM AC or IP-COM router with AP functionality in the network, ensure that the IP address of your computer has been set to 192.168.0.X (X: 2 to 253), and the IP address is not used by any other devices in the same network.
- Clear the cache of your web browser, or replace the web browser.
- Disable the firewall of your computer.
- Replace your computer.
- If two or more APs are connected in the network without an IP-COM AC or IP-COM router with AP functionality, an IP address conflict may happen. You should leave only one AP in the network first and set a new IP address 192.168.0.X (X: 2 to 253) for the AP. Then repeat this procedure to modify the IP addresses of the other APs. Meanwhile, make sure that the IP address of your computer is in the same network segment with your APs' new IP addresses. Then try logging in to the web UI of your APs using their new IP addresses.
- If the AP has been managed by an IP-COM AC or IP-COM router with AP functionality, the AP's IP address may be no longer 192.168.0.254. In that case, go to the web UI of the **AC/router** to view the new IP address of the AP, and then log in to the AP's web UI using the new IP address.
- If the problem persists, reset the AP, and then try logging in again.

**Q2: My access controller (AC) cannot find my AP. What should I do?**

**A2:** Try the following solutions:

- Ensure that all the devices in the network are connected properly and the LED of the AP blinks.
- If VLANs have been defined in your network, verify that the corresponding VLAN has been added to your AP controller.
- Reboot your AP.
- Upgrade firmware your AP to the latest version.
- Reset your AP.

### A.3 Default parameter values

The following table lists the default parameter values of the AP.

Parameter			Default Value
Login	Login IP address		192.168.0.254
	Account	Administrator	User Name/Password: admin/admin (case-sensitive)
		Guest	User Name/Password: user/user (case-sensitive)
Quick Setup	Working Mode		AP
LAN Setup	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)
DHCP Server	DHCP Server		Disable
	Start IP Address		192.168.0.100
	End IP Address		192.168.0.200
	Subnet Mask		255.255.255.0
	Gateway Address		192.168.0.1
	Primary DNS		192.168.0.1
	Lease Time		1 day
SSID	SSID	2.4 GHz	<p>The AP allows 8 SSIDs on the 2.4 GHz band. SSID is IP-COM_XXXXXX. XXXXXX indicates the last 6 digits of the AP's LAN MAC address with a range of XXXXXX~XXXXXX+7.</p> <p>The first (primary) SSID in the drop-down-list box is enabled by default, and the other SSIDs are disabled.</p>
		5 GHz	<p>The AP allows 4 SSIDs on the 5 GHz band. SSID is IP-COM_XXXXXX_5G. XXXXXX indicates the last 6 digits of the AP's LAN MAC address with a range of XXXXXX+8~XXXXXX+B.</p> <p>The first (primary) SSID in the drop-down-list box is enabled by default, and the other SSIDs are disabled.</p>
	Broadcast SSID		Enable
	Isolate Client		Disable

Parameter			Default Value
	Isolate Client		Disable
	WMF		Disable
	Max. Number of Clients		48
	Chinese SSID Encoding		UTF-8
	Security Mode		None
RF Settings	Wireless Network		Enable
	Network Mode	2.4 GHz	11b/g/n
		5 GHz	11ac
	Channel		Auto
	Channel Bandwidth	2.4 GHz	20MHz
		5 GHz	80MHz
	Lock Channel		Enable
	Lock Power		Enable
	Preamble		Long Preamble
	Short GI		Enable
RF Optimization	Suppress Broadcast Probe Response		Disable
	Beacon Interval		100 ms
	Fragment Threshold		2346
	RTS Threshold		2347
	DTIM Interval		1
	RSSI Threshold		-90 dBm
	Signal Transmission		Coverage-oriented
	Prioritize 5 GHz		Disable
	5 GHz Threshold		-80 dBm
	Air Interface Scheduling		Enable
	Anti-interference Mode		3 (Suppress critical interference)
	APSD		Disable
	MU-MIMO		Enable
	Client Timeout Interval		10 minutes
	Mandatory Rate	2.4 GHz	1, 2, 5.5, 11
		5 GHz	6, 12, 24

Parameter			Default Value	
		Optional Rate	2.4GHz	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
			5GHz	6, 9, 12, 18, 24, 36, 48, 54
WMM		No ACK		Disable
		WMM Optimization		Custom
Access Control				Disable
Advanced Settings	Identify Client Type			Disable
	Broadcast Packet Filter			Disable
QVLAN Settings	QVLAN Status			Disable
	PVID			1
	Management VLAN			1
	2.4GHz SSID VLAN ID			1000
	5GHz SSID VLAN ID			1000
Deployment Mode				Local
SNMP	SNMP Agent			Disable
	Administrator			Administrator
	Device Name			Access Point
	Location			ShenZhen
	Read Community			public
	Read/Write Community			private
Tools	Date & Time	System Time		Manual
		Login Timeout Interval		5 minutes
	Log records			150
	Log Service			Disable
	Reboot Schedule			Disable
	LED indicator Control			Enable
	Uplink Detection			Disable