

www.ip-com.com.cn

User Guide

Wireless Access Point

IP-COM
World Wide Wireless

Copyright Statement

©2018 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 with AP325.

Conventions

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

Item	Presentation	Example
Cascading menus	>	System > Live Users
Parameter and value	Bold	Set User Name to Tom .
Variable	Italic	Format: <i>XX:XX:XX:XX:XX:XX</i>
UI control	Bold	On the Policy page, click the OK 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	AP controller
AP	Access Point
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTIM	Delivery Traffic Indication Message
GI	Guard Interval
ISP	Internet Service Provider
PPP	Point to Point Protocol
RF	radio frequency
SSID	Service Set Identifier
VLAN	Virtual Local Area Network

Additional Information

For more information, search this product model on our website at <http://www.ip-com.com.cn>.

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



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

Contents

1 Introduction	1
1.1 Overview	1
1.2 Appearance	1
1.2.1 LED indicator, button, and ports	1
1.2.2 Bottom label	2
2 Installation	4
2.1 Installation procedures	4
3 Quick setup	7
3.1 Overview	7
3.2 Setting up WiFi network without an IP-COM management router/AC	7
3.3 Setting up WiFi network with an IP-COM AP controller	10
3.4 Setting up WiFi network with an IP-COM router supporting AP management	14
4 Login	15
4.1 Logging in to the web UI of the AP	15
4.2 Logging out of the web UI of the AP	16
4.3 Web UI layout	17
4.4 Common buttons	17
5 Status	18
5.1 System status	18
5.2 Wireless status	20
5.3 Traffic statistics	21
5.4 Wireless clients	22
6 Working mode	23
6.1 Overview	23
6.2 Setting WiFi network in AP mode	25
6.3 Setting WiFi network in Client+AP mode	25
7 Network	27
7.1 LAN setup	27
7.2 Changing the LAN IP address of the AP	29
7.2.1 Dynamic IP address	29
7.2.2 Static IP address	29
7.3 DHCP server	31
7.3.1 Overview	31

7.3.2 Configuring the DHCP server	31
7.3.3 DHCP clients.....	32
8 Wireless	34
8.1 Basic.....	34
8.1.1 Overview.....	34
8.1.2 Changing the basic settings	36
8.1.3 Examples.....	39
8.2 RF.....	58
8.2.1 Overview.....	58
8.2.2 Changing the RF settings.....	58
8.3 Radio Optimizing.....	61
8.3.1 Changing the radio optimizing settings	61
8.4 Illegal AP Detection.....	63
8.4.1 Overview.....	63
8.4.2 Scanning wireless signals nearby.....	63
8.5 WMM Setup.....	64
8.5.1 Overview.....	64
8.5.2 Changing the WMM Settings.....	65
8.6 Access Control.....	67
8.6.1 Overview.....	67
8.6.2 Configuring access control.....	67
8.6.3 Example.....	68
8.7 Advanced	70
8.7.1 Overview.....	70
8.7.2 Changing the advanced settings	70
8.8 QVLAN Setup.....	72
8.8.1 Overview.....	72
8.8.2 Configuring the QVLAN function.....	72
8.8.3 Example.....	73
9 SNMP	75
9.1 Overview	75
9.1.1 SNMP management framework	75
9.1.2 Basic SNMP operations.....	75
9.1.3 SNMP protocol version	76
9.1.4 MIB introduction.....	76
9.2 Configuring the SNMP function.....	77
9.3 Example	78
10 Deployment.....	80
10.1 Overview.....	80
10.2 Configuring the deployment mode.....	82
10.2.1 Configuring the local deployment mode.....	82
10.2.2 Configuring the cloud deployment mode.....	82

11 Tools	84
11.1 Firmware Upgrade	84
11.2 Date & Time	85
11.2.1 System Time.....	85
11.2.2 Login Timeout	87
11.3 Logs.....	88
11.3.1 View Logs	88
11.3.2 Configuring log settings	89
11.4 Configuration	92
11.4.1 Backup and restoring configurations	92
11.4.2 Restoring the AP to factory settings	93
11.5 Account.....	95
11.6 Diagnostics Tool	96
11.6.1 Locating the faulty node	96
11.7 Device Reboot.....	97
11.7.1 Manual reboot	97
11.7.2 Automatic reboot.....	97
11.8 LED Control	99
11.9 Uplink Detection	100
11.9.1 Overview	100
11.9.2 Configuring uplink detection	100
Appendix A	102
Appendix B	107
Appendix C	108

1 Introduction

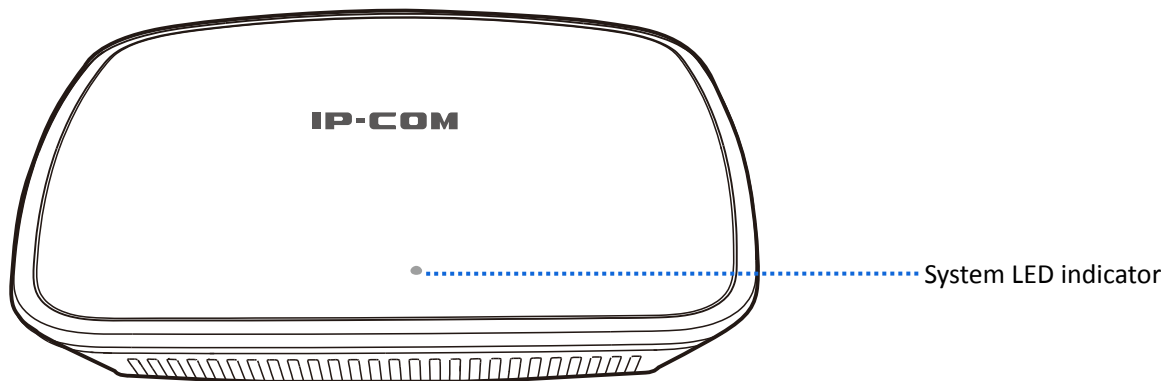
1.1 Overview

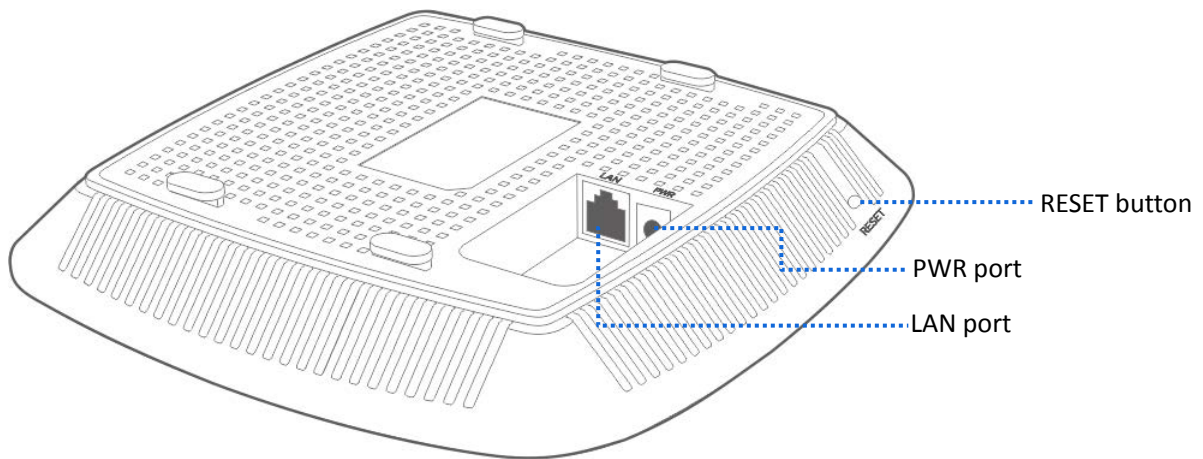
IP-COM wireless access point AP325 operates on 2.4 GHz band and offers a wireless transmission rate as high as 300 Mbps. It can be powered on by DC power supply or IEEE 802.3af/at PoE power supply. Users can manage the AP through its web UI, or by an IP-COM wireless AP controller or an IP-COM router supporting AP controller function. In addition, its ceiling design makes it adaptable to multiple surroundings very well. All in all, AP325 is the right choice for WiFi coverage in hotels and small-and-medium-sized enterprises.

1.2 Appearance

This section describes the LED indicator, button, ports, and bottom label of your AP.

1.2.1 LED indicator, button, and ports





■ **System LED indicator**

System LED indicator	Solid on	<ul style="list-style-type: none">- The system is starting.- If the indicator is still solid on after the AP finishes startup, it indicates that the system is faulty.
	Blinking	The AP is working properly.
	Off	<ul style="list-style-type: none">- The AP is not powered on.- The LED indicator has been turned off.- The AP is faulty.

■ **RESET button**

When the system LED indicator blinks, hold down the RESET button for about 8 seconds. The AP is reset successfully when the system LED indicator gets solid on.

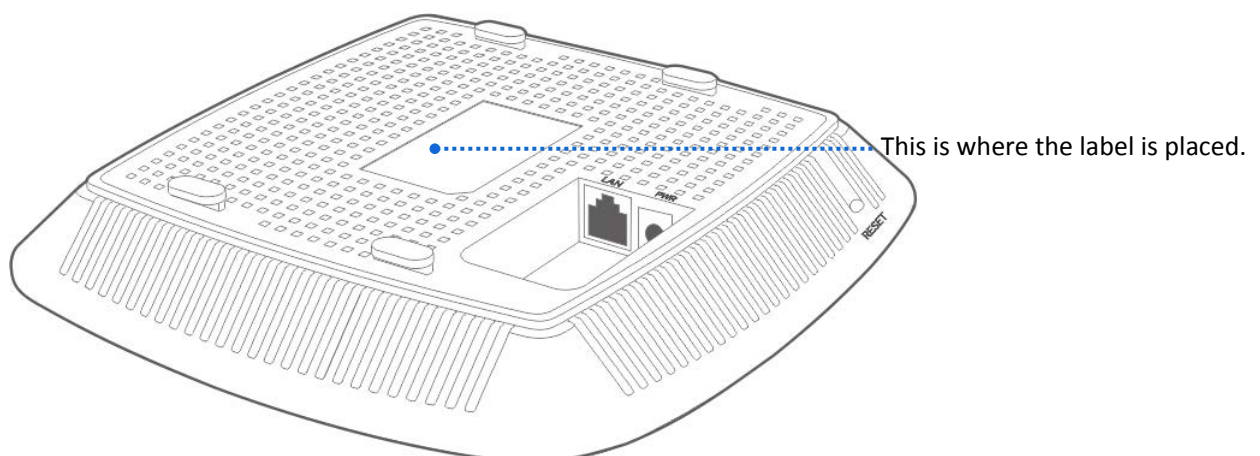
■ **LAN port**

It is a 10/100 Mbps auto-negotiation port used to transmit data or supply IEEE 802.3af/at PoE power for the AP using an Ethernet cable. You can connect this port to a router or a PoE switch.

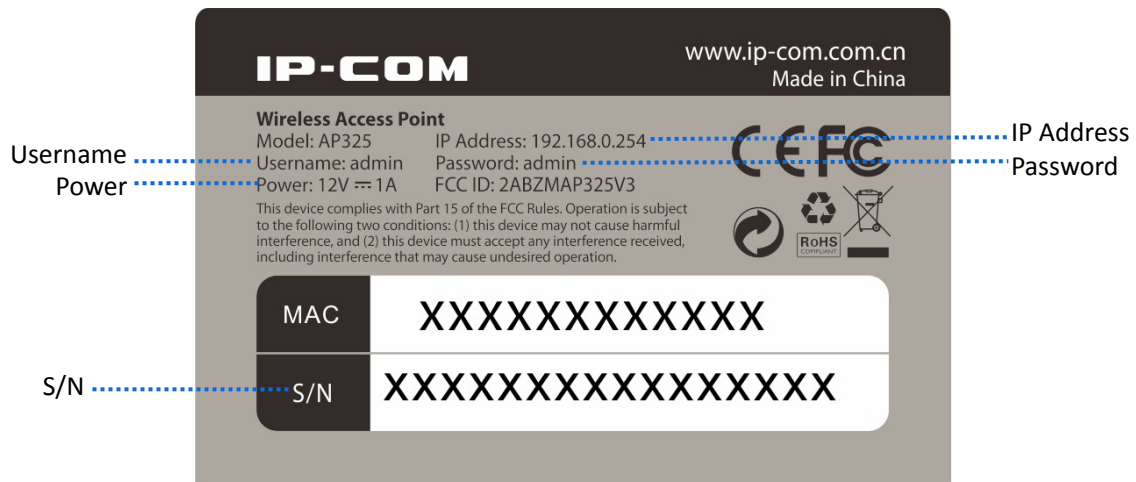
■ **PWR port**

It is a power port used to connect to a DC power resource using the power adapter included in the package.

1.2.2 Bottom label



The bottom label shows the AP's default IP address, login username and password, input DC power supply, and serial number. See the following figure:



IP Address: It specifies the default IP address of the AP. You can use this IP address to log in to your AP's web UI when you set it for the first time. After you change the IP address, you should use the new IP address to log in to its web UI.

Username/Password: It specifies the default login username/password used to log in to the web UI of the AP. After you change the username/password, you should use the new username/password to log in to its web UI.

Power: It specifies the input DC power supply of the AP.

S/N: It specifies the serial number of the AP. If the AP is faulty, you need to provide this serial number for repair.

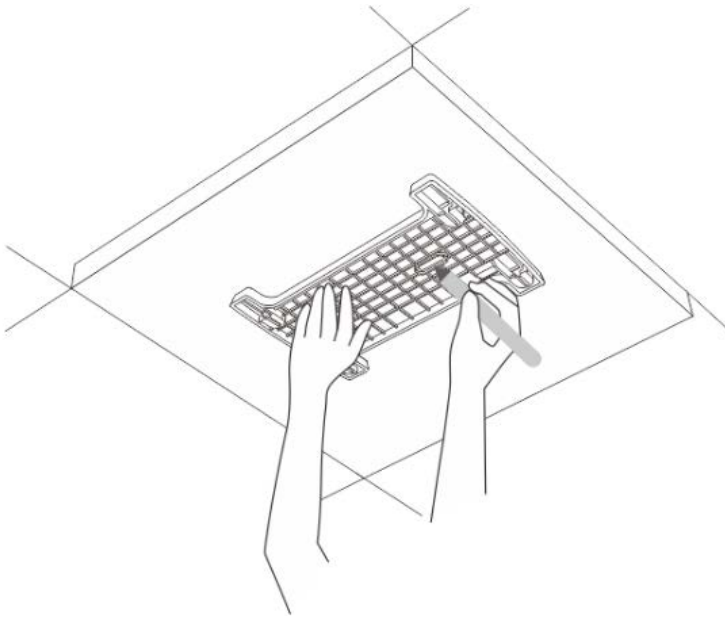
2 Installation

2.1 Installation procedures

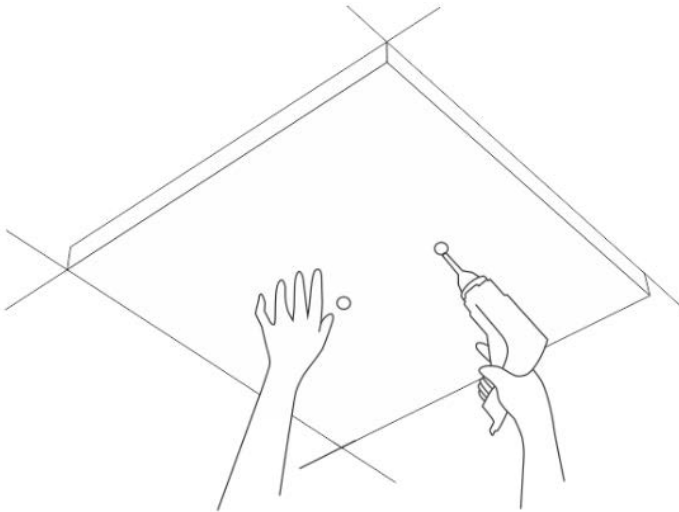


Before installing the AP onto your ceiling, you should prepare a rubber hammer, a marker, a hammer drill, a drill bit, a screwdriver, and a ladder for installation.

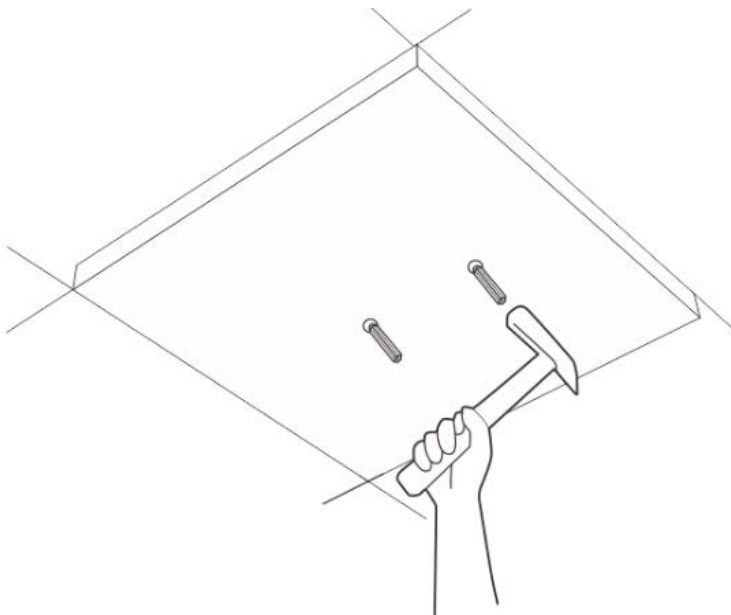
1. Position the bracket on the ceiling and mark screw holes on the ceiling with the marker.



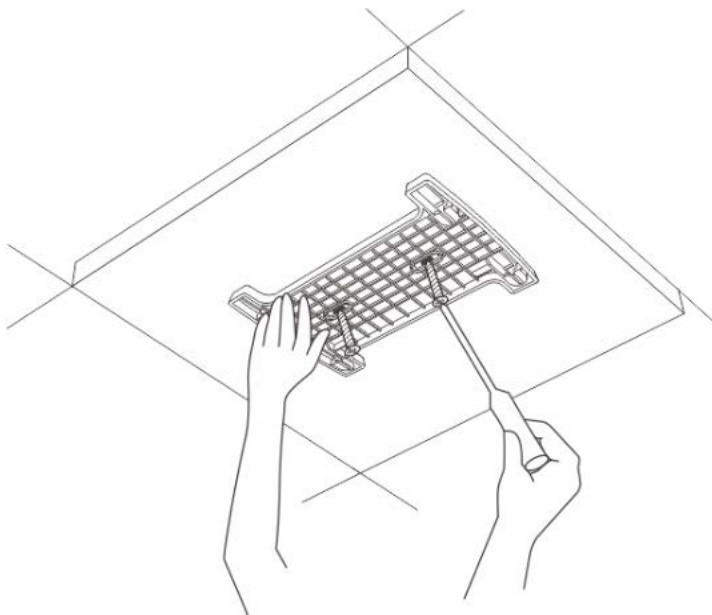
2. Drill holes in the marked positions using a hammer drill.



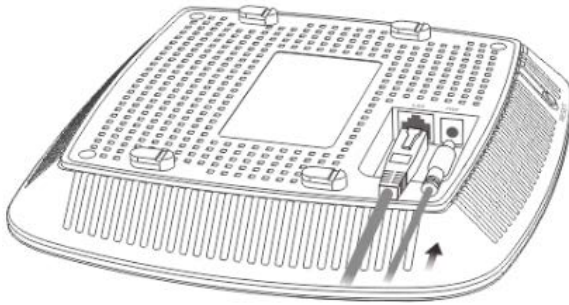
3. Knock the expansion bolts into the holes using a rubber hammer.



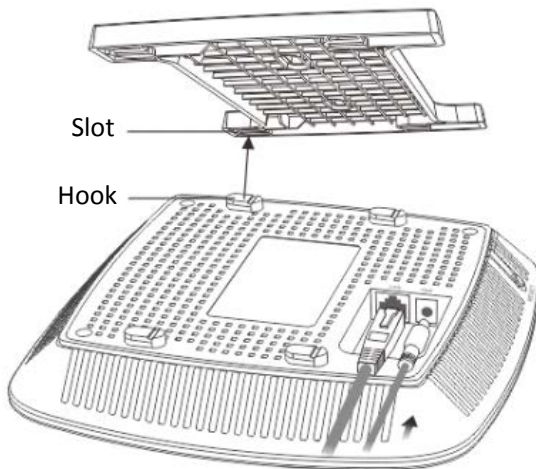
4. Use the screwdriver to drive screws into the expansion bolts so as to fasten the bracket.



5. Connect an Ethernet cable (CAT5 or better) to the LAN port of the AP. If you choose to power on the AP by DC power supply, connect the PWR port of the AP to a power resource using the power adapter included in the package.



6. Insert the hooks of the AP into the slots of the bracket, and slide the AP to one side to make the AP is fixed well in the bracket.



---End

3 Quick setup

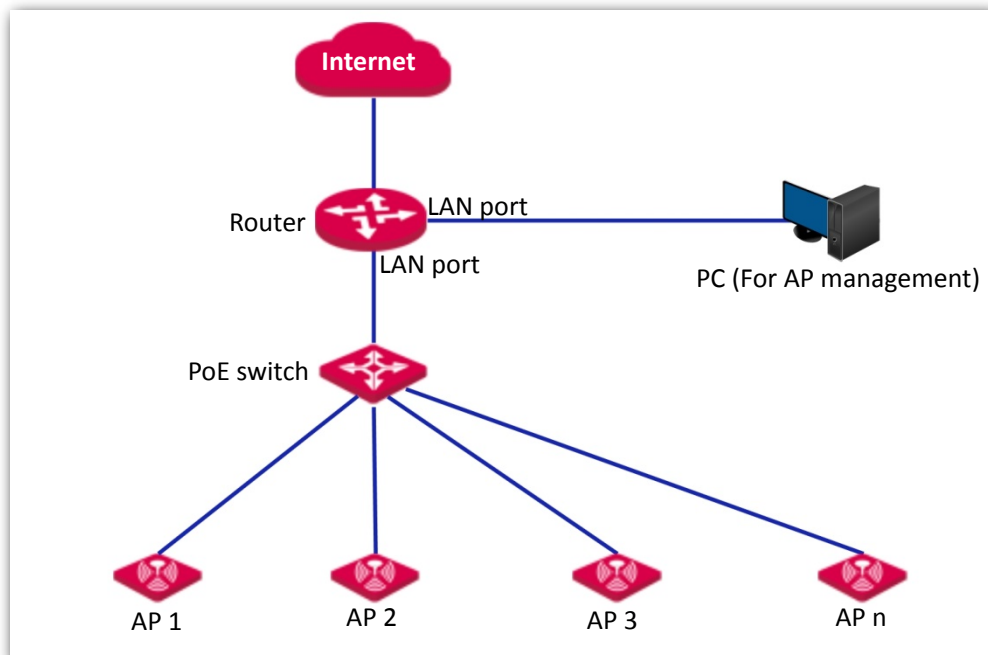
3.1 Overview

This chapter is about how to set up WiFi network for APs in different scenarios. Please select one method for internet setup according to your scenario.

3.2 Setting up WiFi network without an IP-COM management router/AC


1. Connect devices.
 - (1) Ensure that your router is connected to the internet.
 - (2) Ensure that your router and PoE switch are connected to power supply.
 - (3) Connect your computer and PoE switch to LAN ports of the router using Ethernet cables.
 - (4) Connect LAN port of your AP to a PoE port of your PoE switch using an Ethernet cable.

The network topology is shown as follows:

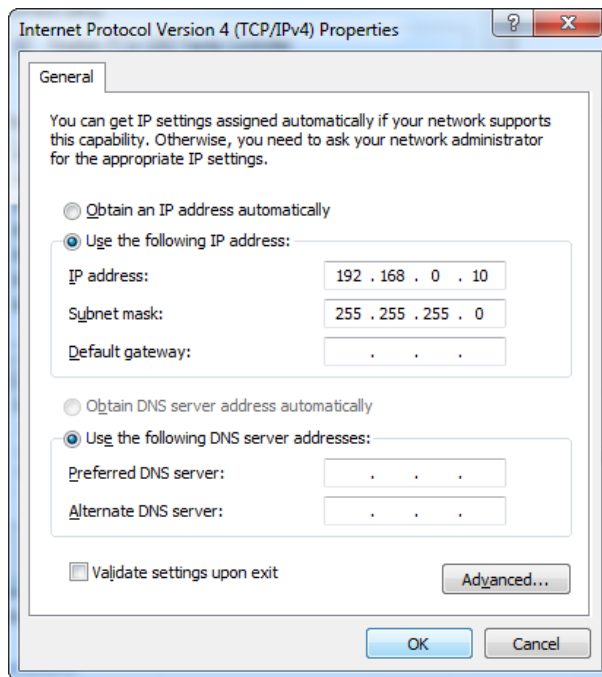




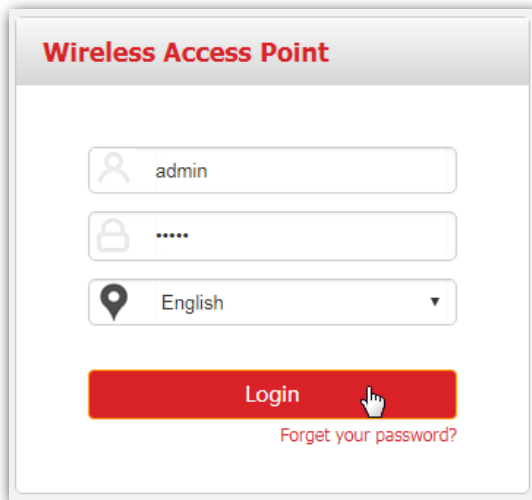
- If you choose to power on your AP using DC power supply, connect the PWR port of your AP to a DC power resource using the included power adapter.
- If you have several IP-COM APs, to avoid IP address conflict, you should connect one AP to a PoE port of your PoE switch first and set a new IP address for the AP. Then repeat this procedure to connect other APs one by one and configure new IP addresses for them respectively.

After finishing connection, ensure that the AP's LED indicator blinks and the lower-right network icon on your computer is not displayed .

2. Configure the IP address of your computer (Example: Win7).
 - (1) Right-click the network icon on the lower-right corner of your computer. Then click **Open Network and Sharing Center, Local Area Connection, and Properties**.
 - (2) Double-click **Internet Protocol Version 4 (TCP/IPv4)**, select **Use the following IP address**, set **IP address** to **192.168.0.x** (x: 2 to 253. The IP address in this example is 192.168.0.10) and **Subnet mask** to **255.255.255.0**.
 - (3) Click **OK**.

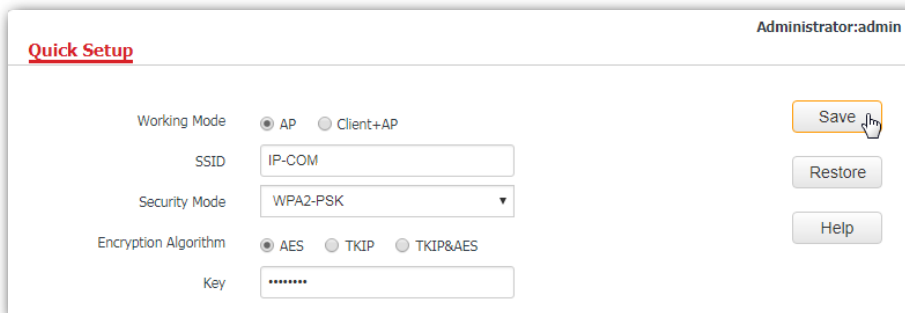


3. Log in to the web UI of your AP.
 - (1) Start a web browser on your computer. Enter **192.168.0.254** in the address bar, and press **Enter**.
 - (2) Enter the user name and password (default: **admin/admin**) of the AP.
 - (3) Click **Login**.



4. Set SSID (WiFi name) and key (password) for your AP's WiFi network.

- (1) To access the configuration page, click **Quick Setup**.
- (2) **SSID, Security Mode, Key:** Set an **SSID**, **Security Mode** (WPA2-PSK is recommended), and **Key** for your AP manually.
- (3) Click **Save**.



5. Change the IP address of your AP.

- (1) To access the configuration page, click **Network > LAN Setup**.
- (2) **IP Address:** Change the IP address of the AP to 192.168.0.x (x: 2 to 253), which is **192.168.0.250** in this example.
- (3) Click **Save**.

LAN Setup Administrator:admin

MAC Address 00:90:4C:88:88:88

IP Address Type Static

IP Address 192.168.0.250 Example: 192.168.1.254

Subnet Mask 255.255.255.0 Example: 255.255.255.0

Gateway 192.168.0.1

Primary DNS Server 8.8.8.8

Secondary DNS Server 8.8.4.4 (optional)

Device Name Wireless Access Point

Driving Capability of Port Standard Enhanced (lower port speed)

Save Restore Help

Wait a moment to apply the settings.

6. Connect your wireless devices like smart phones to your AP's WiFi network using the WiFi name and password you set in step 4.

 **Note**

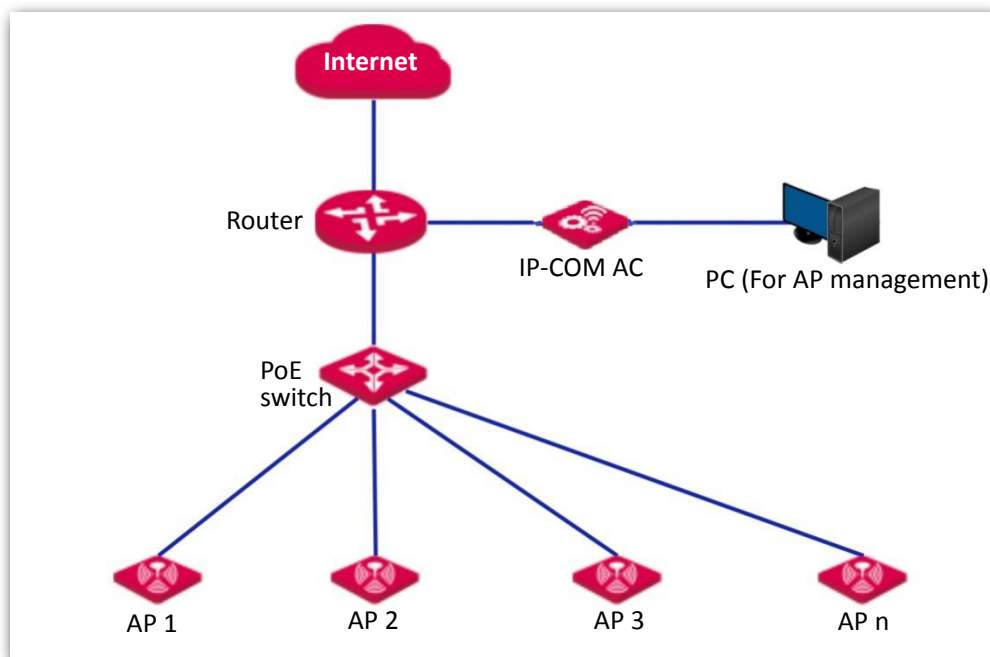
The new IP address you set for the AP should not be used by other devices in the same LAN network, and the IP address of your management computer should be in the same network segment as the new IP address.

---End

3.3 Setting up WiFi network with an IP-COM AP controller


A hotel may be deployed with lots of APs. But you can use an IP-COM AP controller (AC) to manage the APs centrally. The following describes the procedures.

1. Connect devices.
 - (1) Ensure that your router is connected to the internet.
 - (2) Ensure that your router, PoE switch and AC are connected to power supply.
 - (3) Connect your IP-COM AC and PoE switch to LAN ports of your router using Ethernet cables. IP-COM AC2000 is used for instructions in this example.
 - (4) Connect your APs to PoE ports of your PoE switch using Ethernet cables.
 - (5) Connect your computer to a port of your AC.

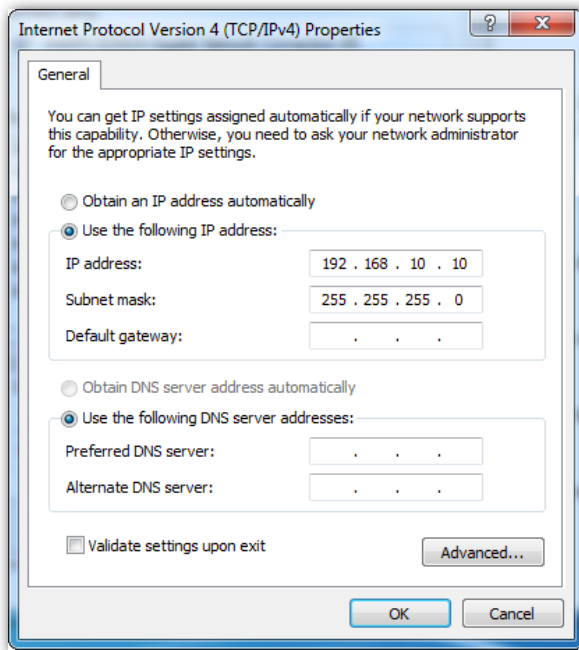


Note

If you choose to power on your AP using DC power supply, connect the PWR port of your AP to a DC power resource using the included power adapter.

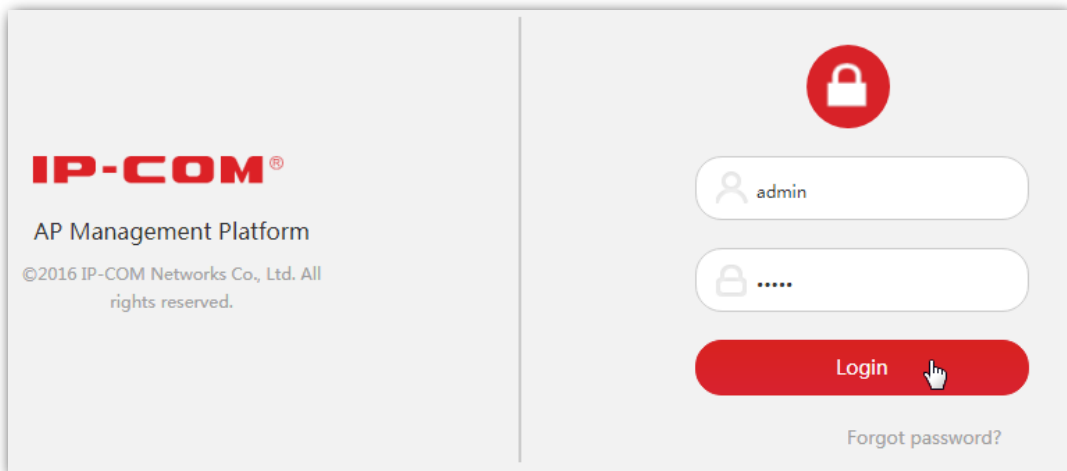
After finishing connection, ensure that the AP's LED indicator blinks and the lower-right network icon on your computer is not displayed .

2. Set the IP address of your computer (Example: Windows 7)
 - (1) Right-click the network icon on the lower-right corner of your computer. Then click **Open Network and Sharing Center, Local Area Connection, and Properties**.
 - (2) Double-click **Internet Protocol Version 4 (TCP/IPv4)**, select **Use the following IP address**, set **IP address** to **192.168.10.x** (x: 2 to 253. The IP address in this example is 192.168.10.10) and **Subnet mask** to **255.255.255.0**.
 - (3) Click **OK**.



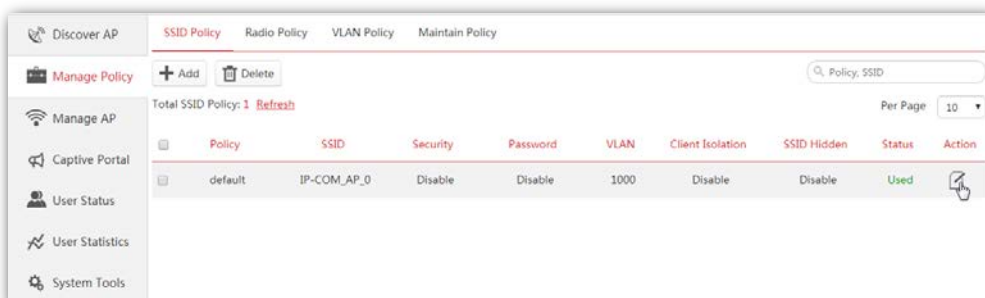
3. Log in to the web UI of the AC.

- (1) Start a web browser on the computer connected to the AC, enter the management IP address of the AC (default: **192.168.10.1**) in the address bar, and press **Enter**.
- (2) Enter the user name and password of the AC (default user name and password: **admin/admin**) and click **Login**.



4. Configure the APs.

- (1) To access the configuration page, choose **Manage Policy**. Then click  to access the detailed configuration page.



- (2) **SSID, Security and Key:** Set an SSID (WiFi name), security, key (WiFi password) for your AP, and click **Save** to apply the settings.

SSID Policy

Policy: default

SSID: IP-COM_AP_1

Security: WPA2-PSK

Encryption: AES TKIP TKIP&AES

Key: 12345678

Key interval: 0 S

Client Limit For SSID: 64

Client Isolation: Enable

SSID Hidden: Enable

VLAN ID: 1000

Note : VLAN ID for SSID tagging only be activated after VLAN Policy enabled on the access Point

Save Cancel

Wait a minute. The AP will obtain the WiFi settings from the AC automatically. You can view your AP's new SSID and IP address on the **Discover AP** page.

Discover AP

Online APs: 1 Refresh

Model	Remark	IP	MAC	Online User	SSID	Channel	Version	Status
AP325V3.0	Wireless A...	192.168.10.115	00:90:4C:88:88:88	0	IP-COM_AP_1	5	V1.0.0.2(1195)	Online

5. Connect your wireless devices like smart phones to your AP's WiFi network using the WiFi name and password you set in step 4.

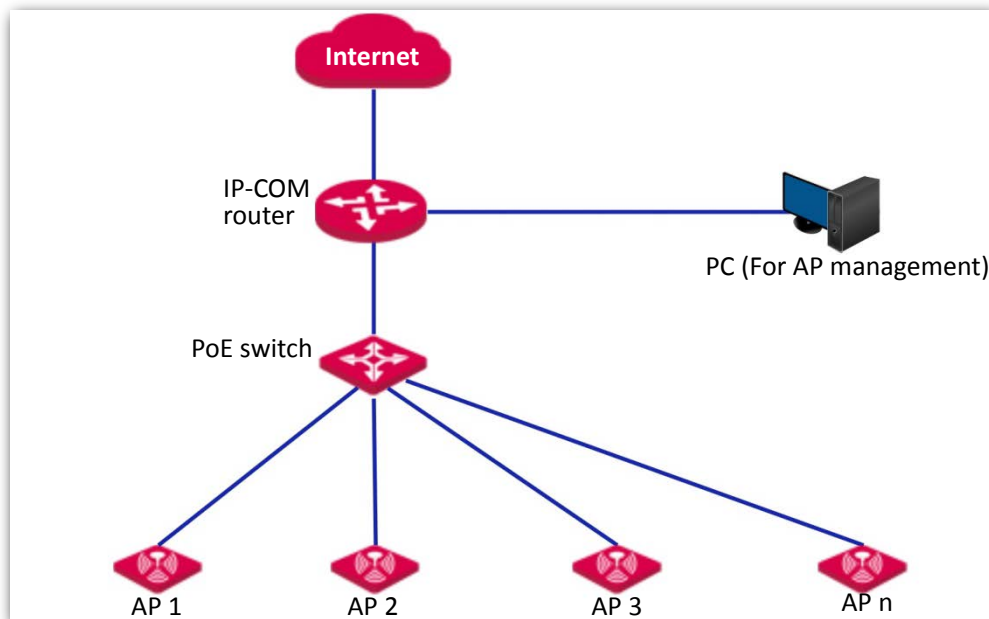
---End

3.4 Setting up WiFi network with an IP-COM router supporting AP management

A hotel may be deployed with a large number of APs. But you can manage them centrally using IP-COM router supporting AP management. The following describes the procedure.


1. Connect devices.
 - (1) Ensure that your IP-COM router is connected to the internet.
 - (2) Ensure that your router and PoE switch are connected to power supply.
 - (3) Connect your computer and PoE switch to the LAN ports of the router using Ethernet cables.
 - (4) Connect your APs to PoE ports of your PoE switch using Ethernet cables.

The network topology is shown as follows:



Note

If you choose to power on your AP using DC power supply, connect the PWR port of your AP to a DC power resource using the included power adapter.

After finishing connection, ensure that the AP's LED indicator blinks and the lower-right network icon on your computer is not displayed .

2. Start a web browser on your computer and log in to the web UI of the router. For details about managing your APs, refer to your router's user guide.

---End

Note

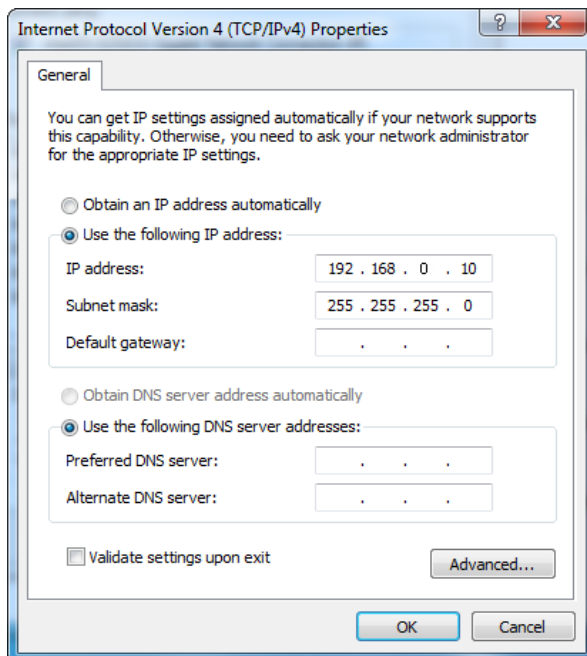
If your AP is managed by an IP-COM router in the LAN network, the AP's IP address may have been changed. If you want to go to the AP's web UI, first view the new IP address of the AP on the web UI of the router, then log in to the AP's web UI using the new IP address.

4 Login

4.1 Logging in to the web UI of the AP

If you want to log in to the web UI of your AP, perform the following procedures:

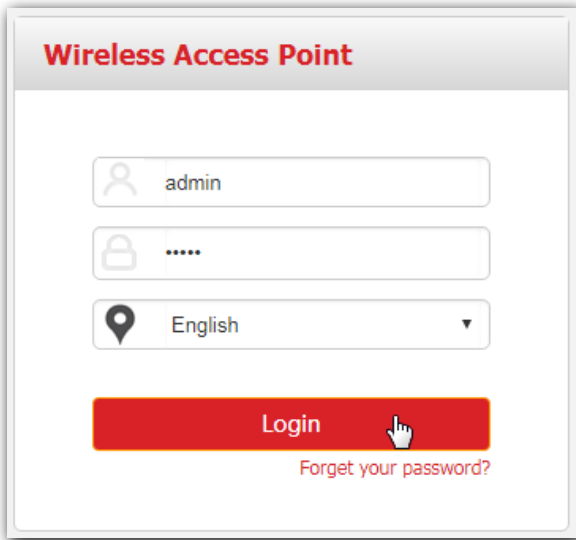
1. Connect your management computer to the AP' WiFi network or the PoE switch connected to the AP using an Ethernet cable.
2. Set IP address of your computer to **192.168.0.X** (X: 2 - 253) and subnet mask to **255.255.255.0**.



Note

If your AP is managed by an IP-COM AC/router in the LAN network, the AP's IP address may have been changed. In that case, go to the web UI of the router/AC to view the new IP address of the AP, set the IP address of your computer in the same network segment as the AP's new IP address, then log in to the AP's web UI using the new IP address.

3. 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**.
4. Enter the user name and password of the AP (default user name and password: **admin/admin**) and press **Login**.

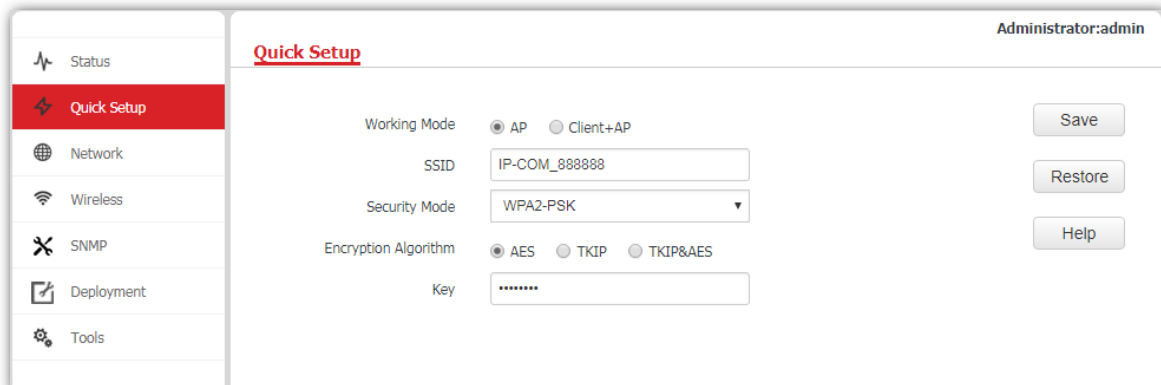


Note

If your AP's login page does not appear, refer to **Q1** in **Appendix B**.

---End

Log in to the web UI of the AP successfully. See the following figure:

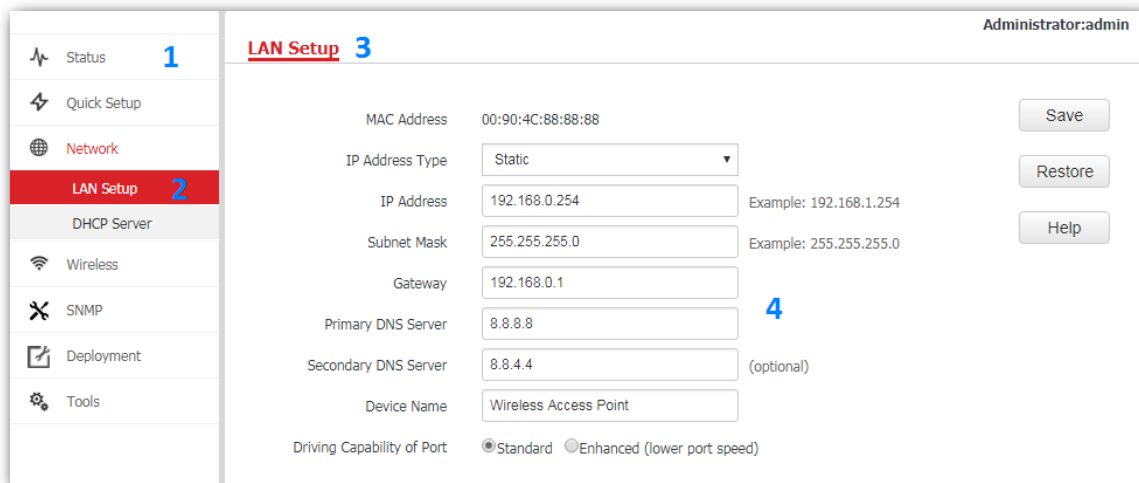


4.2 Logging out of the web UI of the AP

When you close the web browser, the system logs you out automatically, or if you log in to the web UI of the AP but perform no operation within the login timeout interval, the AP logs you out as well. The default login timeout interval of the AP is 5 minutes, and you can configure it yourself on the page **Tools > Date & Time > Login Timeout**.

4.3 Web UI layout

The web UI of the AP is composed of four parts, including the navigation trees of two levels, tab page area, and configuration area. See the following figure.



No.	Name	Description
1	Level-1 navigation bar	The navigation bars and tab pages display the function menu of the AP. When you select a function in the navigation bar, the corresponding configuration appears in the configuration area.
2	Level-2 navigation bar	
3	Tab page area	
4	Configuration area	In this area, you can view and modify configuration of the AP.



The functions and parameters dimmed on the web UI indicates that they cannot be changed in the current configuration or they are not supported by the AP. If you want to configure the functions or parameters dimmed on the web UI, you need to configure their related functions or parameters on the web UI first.

4.4 Common buttons

The following table describes the common buttons available on the web UI of the AP.

Button	Description
Save	Click it to save the configuration on the current page and enable the configuration to take effect.
Restore	Click it to set the configuration on the current page back to the original configuration.
Help	Click it to view corresponding help information on the page.

5 Status

5.1 System status

This page displays the system status and LAN port status of the AP. To access the page, click **Status > System Status**.

The screenshot displays the 'System Status' page. On the left is a sidebar with navigation items: Status, System Status (highlighted), Wireless Status, Traffic Statistics, Wireless Clients, Quick Setup, Network, Wireless, SNMP, Deployment, and Tools. The main content area is titled 'System Status' and includes a 'Help' button. It lists the following parameters:

- System Status**
 - Device Name: Wireless Access Point
 - System Time: 2018-05-11 16:06:25
 - Uptime: 00h41m29s
 - Number of Clients: 0
 - Firmware Version: V1.0.0.2(1195)
 - Hardware Version: V3.0
- LAN Status**
 - MAC Address: 00:90:4C:88:88:88
 - IP Address: 192.168.0.254
 - Subnet Mask: 255.255.255.0
 - Primary DNS Server: 8.8.8.8
 - Secondary DNS Server: 8.8.4.4

Parameter description

Parameter	Description
Device Name	It specifies the name of the AP. You can change the AP's name on Network > LAN Setup page.
System Time	It specifies the current system time of the AP.
Uptime	It specifies the time that has elapsed since the AP starts up this time.
Number of Clients	It specifies the number of wireless devices connected to the AP currently.
Firmware Version	It specifies the current firmware version number of the AP. If you have upgraded the firmware version of the AP, view the current firmware version here to check whether the upgrade is successful.
Hardware Version	It specifies the current hardware version number of the AP.
MAC Address	It specifies the physical address of the AP's LAN port. If you connect the AP to

Parameter	Description
	other devices using Ethernet cables, the AP uses this MAC address to communicate with those devices.
IP Address	It specifies the AP's IP address used to log in to its web UI. If you want to change the IP address, access the Network > LAN Setup page and perform according to the on-screen instructions.
Subnet Mask	It specifies the subnet mask of the AP's IP address.
Primary DNS Server	It specifies the primary DNS server of the AP.
Secondary DNS Server	It specifies the secondary DNS server of the AP.

5.2 Wireless status

This page displays radio frequency and SSID status of the AP. To access the page, click **Status > Wireless Status**.

The screenshot shows the 'Wireless Status' page. The top right corner indicates 'Administrator:admin'. The page is divided into two main sections: 'RF Status' and 'SSID Status'. The 'RF Status' section contains a table with three rows: 'RF (On/Off)' set to 'On', 'Network Mode' set to 'b/g/n', and 'Channel' set to '2'. The 'SSID Status' section contains a table with four columns: 'SSID', 'MAC Address', 'Enabled/Disabled', and 'Security Mode'. It lists four SSIDs: 'IP-COM_888888' (Enabled, WPA2-PSK), 'IP-COM_888889' (Disabled, None), 'IP-COM_88888A' (Disabled, None), and 'IP-COM_88888B' (Disabled, None). A 'Help' button is visible on the right side of the RF Status table.

Parameter description

Parameter	Description	
RF(On/Off)	It specifies whether the RF (radio frequency) function of the AP is enabled. On represents the RF is enabled, and Off is disabled. You can change the RF status on the Wireless > RF page.	
RF Status	Network Mode	It specifies the current network mode of the AP. You can change the network mode on the Wireless > RF page.
	Channel	It specifies the current working channel of the AP. You can change the working channel on the Wireless > RF page.
SSID Status	SSID	It specifies the names of all WiFi networks of the AP. The AP supports four WiFi networks at most. The first SSID in the SSID status table is the primary SSID. By default, the WiFi network corresponding to the primary SSID is enabled, and the other three WiFi networks are disabled.
	MAC Address	It specifies the physical address of the corresponding SSID.
	Enabled/Disabled	It specifies whether the corresponding WiFi network is enabled.
	Security Mode	It specifies the security mode of the corresponding WiFi network.

5.3 Traffic statistics

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

This page displays statistics about historical packets of AP's WiFi network. To access the page, click **Status > Traffic Statistics**.

Administrator:admin

Traffic Statistics

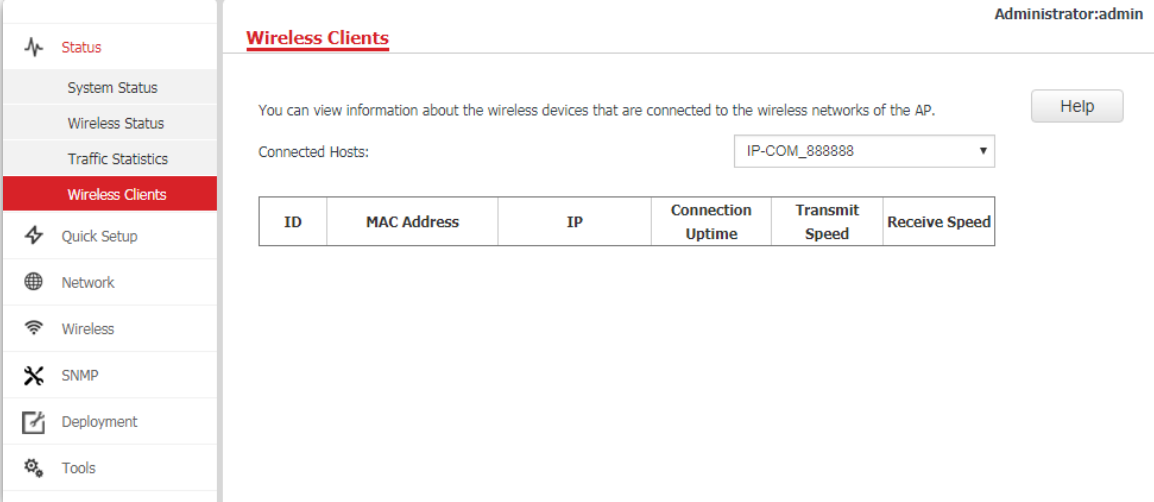
SSID	Received Traffic	Received Packets	Transmitted Traffic	Transmitted Packets
IP-COM_888888	29.37MB	122226	0.06MB	242
IP-COM_888889	0.00MB	0	0.00MB	0
IP-COM_88888A	0.00MB	0	0.00MB	0
IP-COM_88888B	0.00MB	0	0.00MB	0

Help

Refresh

5.4 Wireless clients

This page displays information about the wireless devices connected to AP's WiFi networks. To access the page, click **Status > Wireless Clients**.



The screenshot shows a web interface for managing a wireless access point. On the left is a navigation menu with items: Status, System Status, Wireless Status, Traffic Statistics, **Wireless Clients** (highlighted), Quick Setup, Network, Wireless, SNMP, Deployment, and Tools. The main content area is titled "Wireless Clients" and includes a "Help" button. Below the title, there is a text box stating: "You can view information about the wireless devices that are connected to the wireless networks of the AP." Underneath, there is a "Connected Hosts:" label and a drop-down menu currently showing "IP-COM_888888". At the bottom of the main area is a table with the following headers: ID, MAC Address, IP, Connection Uptime, Transmit Speed, and Receive Speed.

By default, this page displays information about the wireless devices connected to the primary WiFi network. To view information about the wireless devices connected to the other three WiFi networks, select the SSIDs from the drop-down list box.

6 Working mode

6.1 Overview

This chapter is mainly about your AP's working mode: AP and Client+AP. To access the configuration page, click **Quick Setup**. See the following figure.

The screenshot shows the 'Quick Setup' configuration page. On the left is a navigation menu with 'Quick Setup' selected. The main area contains the following settings:

- Working Mode: AP Client+AP
- SSID:
- Security Mode: - Encryption Algorithm: AES TKIP TKIP&AES
- Key:

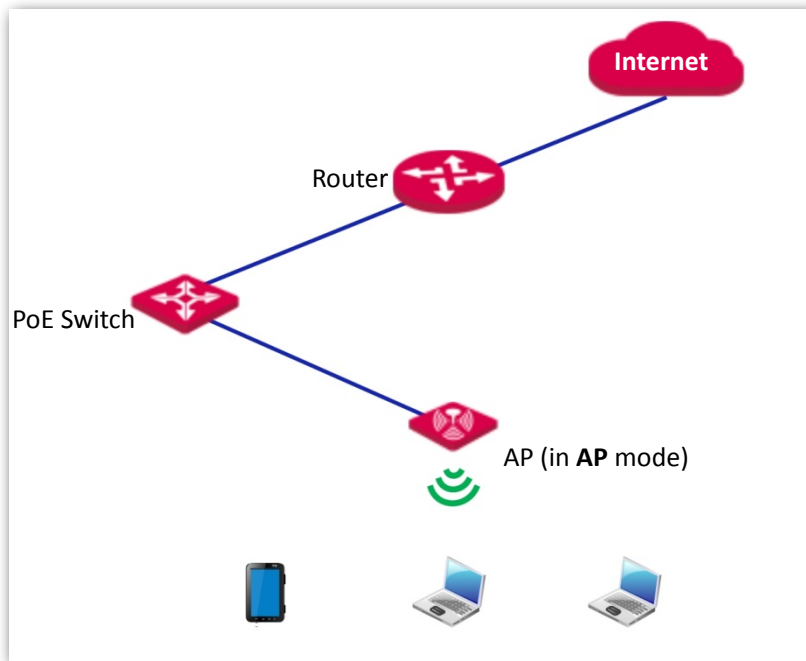
Buttons for 'Save', 'Restore', and 'Help' are on the right. The top right corner shows 'Administrator:admin'.

Parameter description

Parameter	Description
Working Mode	It specifies the working mode you set for your AP, including AP mode and Client+AP mode.
SSID	It specifies the SSID (WiFi name) you set for your AP.
Security Mode	It specifies the security mode you set for your AP's WiFi network, including None , WEP , WPA-PSK , WPA2-PSK , Mixed WPA/WPA2-PSK , WPA and WPA2 .
Key	It specifies the WiFi password you set for your AP's WiFi network.

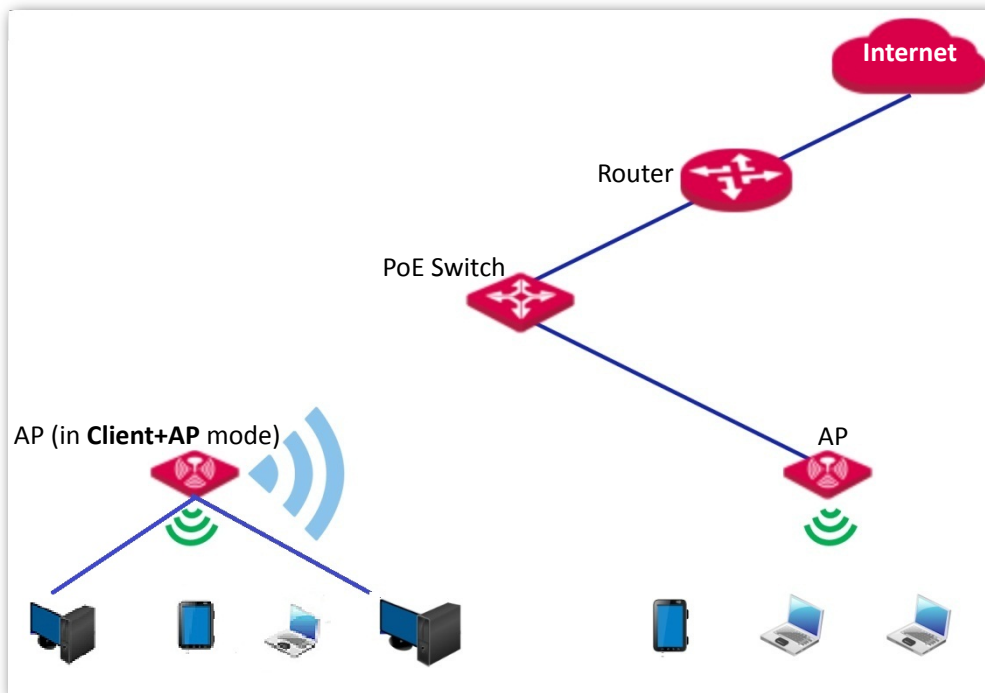
■ AP mode

By default, the AP works in AP mode. In this mode, the AP connects to an upstream device (such as a router or PoE switch) using an Ethernet cable and converts wired signal into wireless one to offer WiFi coverage. See the following topology.



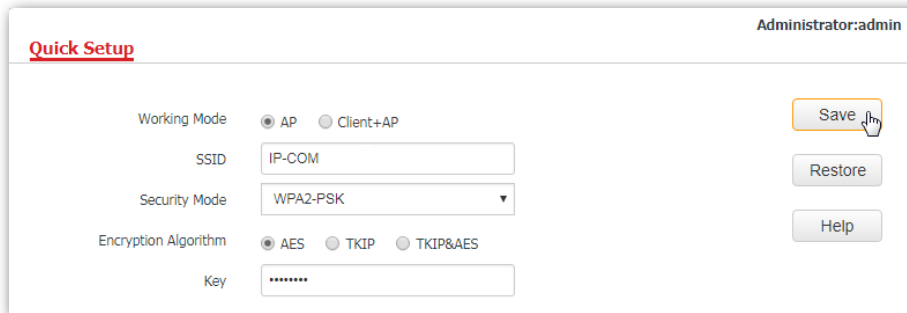
■ **Client+AP mode**

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



6.2 Setting WiFi network in AP mode

1. Click **Quick Setup**.
2. **Working Mode**: Select **AP** mode.
3. **SSID**: Set a WiFi name for your AP's WiFi network, which is IP-COM_83F4B0 in this example.
4. **Security Mode**: Select one security mode for your AP. You are recommended to select **WPA2-PSK**.
5. **Encryption Algorithm**: Select one encryption algorithm for your AP, which is **AES** in this example.
6. **Key**: Set a WiFi password for your AP's WiFi network.
7. Click **Save**.



The screenshot shows the 'Quick Setup' page for an administrator. The page title is 'Quick Setup' and the user is 'Administrator:admin'. The 'Working Mode' is set to 'AP'. The 'SSID' is 'IP-COM'. The 'Security Mode' is 'WPA2-PSK'. The 'Encryption Algorithm' is 'AES'. The 'Key' is masked with dots. There are three buttons on the right: 'Save', 'Restore', and 'Help'. The 'Save' button is highlighted with a yellow box and a mouse cursor.

---End

After configuration, connect wireless devices to your AP's WiFi network using the SSID and WiFi password you set on the **Quick Setup** page.

6.3 Setting WiFi network in Client+AP mode

1. Click **Quick Setup**.
2. **Working Mode**: Click **Client+AP** mode.
3. Click **Scan**.
4. Select the WiFi network you want to extend from the WiFi network list that appears, which is **Tom-WiFi** in this example.

Note

- If no WiFi network is found, click **Wireless > RF** to ensure that **Enable RF** is selected, and try scanning again.
 - After a WiFi network is selected, the AP identifies its SSID, security mode, encryption algorithm, channel of WiFi network and populates them on the page automatically. However, some other parameters such as **Key** must be entered yourself.
-

Administrator:admin

Quick Setup

Working Mode AP Client+AP Save

SSID Restore

Security Mode Help

Encryption Algorithm AES TKIP TKIP&AES

Key

Upstream AP Channel Disable Scan

Select	SSID	MAC Address	Network Mode	Channel Bandwidth	Channel	Extension Channel	Security Mode	Signal Strength
<input checked="" type="radio"/>	Tom-WiFi	c8:3a:35:83:fd:01	bgn	40	8	lower	wpa&wpa2/ae...	-22dBm
<input type="radio"/>	IP-COM_1	50:2b:7b:ff:30:89	bgn	40	6	upper	wpa&wpa2/ae...	-48dBm
<input type="radio"/>	MW3_test	b4:0f:3b:43:d8:61	bgn	40	6	upper	wpa&wpa2/ae...	-50dBm

- If the WiFi network of the upstream device is encrypted, enter the WiFi password of the upstream device's in the **Key** box. Click **Save**.

Administrator:admin

Quick Setup

Working Mode AP Client+AP Save

SSID Restore

Security Mode Help

Encryption Algorithm AES TKIP TKIP&AES

Key

Upstream AP Channel Disable Scan

Select	SSID	MAC Address	Network Mode	Channel Bandwidth	Channel	Extension Channel	Security Mode	Signal Strength
<input checked="" type="radio"/>	Tom-WiFi	c8:3a:35:83:fd:01	bgn	40	8	lower	wpa&wpa2/ae...	-22dBm
<input type="radio"/>	IP-COM_1	50:2b:7b:ff:30:89	bgn	40	6	upper	wpa&wpa2/ae...	-48dBm
<input type="radio"/>	MW3_test	b4:0f:3b:43:d8:61	bgn	40	6	upper	wpa&wpa2/ae...	-50dBm

---End

After the configuration, your computer connected to the AP can access the internet directly. And you can also connect wireless devices to the AP's WiFi network using the AP's own SSID and WiFi password. If you do not know the SSID of the AP, click **Wireless > Basic**.

7 Network

7.1 LAN setup

This page enables you to check the MAC address of your AP's LAN port, set the LAN port's IP address type and other parameters. To access the page, click **Network > LAN Setup**.

The screenshot shows the 'LAN Setup' configuration page. At the top right, it says 'Administrator:admin'. The page title is 'LAN Setup'. The form contains the following fields and values:

- MAC Address: 00:90:4C:88:88:88
- IP Address Type: Static (dropdown menu)
- IP Address: 192.168.0.254 (Example: 192.168.1.254)
- Subnet Mask: 255.255.255.0 (Example: 255.255.255.0)
- Gateway: 192.168.0.1
- Primary DNS Server: 8.8.8.8
- Secondary DNS Server: 8.8.4.4 (optional)
- Device Name: Wireless Access Point
- Driving Capability of Port: Standard Enhanced (lower port speed)

Buttons for 'Save', 'Restore', and 'Help' are located on the right side of the form.

Parameter description

Parameter	Description
MAC Address	It specifies the MAC address of the AP's LAN port.
IP Address Type	It specifies how the AP gets its IP address. The default option is Static . <ul style="list-style-type: none">– Static: It indicates that the AP has static IP address information. In this condition, you need to set IP address, subnet mask, gateway, and DNS server information for the AP manually.– Dynamic: It indicates that the AP gets IP address, subnet mask, gateway, and DNS server information from a DHCP server in your LAN network automatically.



Tip

If **IP Address Type** is set to **Dynamic**, you should log in to the web UI of the AP using the AP's dynamic IP address assigned by the DHCP server. To get the AP's dynamic

Parameter	Description
	IP address, find it in the client list of the DHCP server.
IP Address	It specifies the IP address of the AP (default: 192.168.0.254). You can access the web UI of the AP using this IP address.
Subnet Mask	It specifies the subnet mask of the IP address of the AP. The default subnet mask is 255.255.255.0 .
Gateway	It specifies the gateway IP address of the AP. Generally, to ensure that the AP can access the internet successfully, you should set the gateway IP address to the LAN IP address of the LAN router connected to the internet.
Primary DNS Server	It specifies the IP address of the primary DNS server of the AP. If DNS proxy function is supported on your LAN 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.
Secondary DNS Server	It specifies the IP address of the secondary DNS server of the AP. This parameter is optional.
Device Name	It specifies the name of the AP.
Driving Capability of Port	It specifies the LAN port's driving mode, including Standard and Enhanced . <ul style="list-style-type: none">– Standard: In this mode, the LAN port supports a higher transmission speed but a shorter transmission distance. In general, you are recommended to select this mode.– Enhanced: In this mode, the LAN port supports a longer transmission distance but a lower transmission speed, such as 10 Mbps.

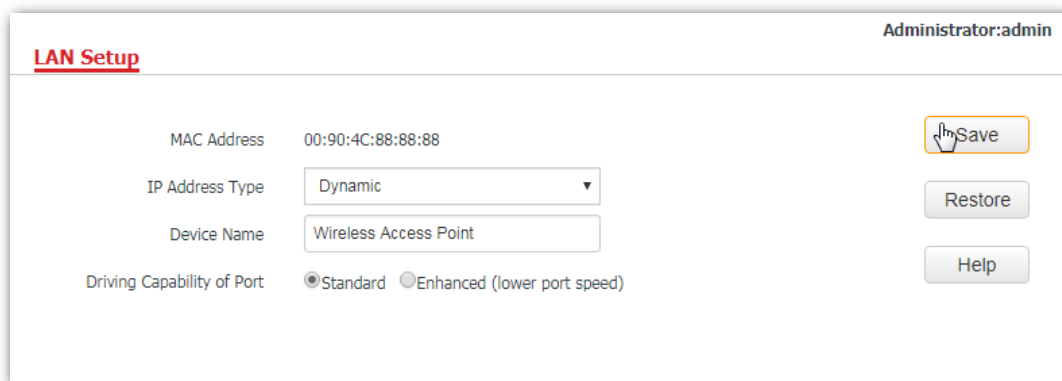
7.2 Changing the LAN IP address of the AP

7.2.1 Dynamic IP address

This IP address type enables your AP to obtain an IP address, a subnet mask, a gateway IP address, DNS server IP addresses from a LAN DHCP server automatically. If a large number of APs are deployed, you are recommended to adopt this type to prevent IP address conflicts and reduce your workload.

Procedure:

1. To access the configuration page, click **Network > LAN Setup**.
2. Set **IP Address Type** to **Dynamic**.
3. Click **Save**.



The screenshot shows the 'LAN Setup' configuration page. At the top right, it says 'Administrator:admin'. The page has a title 'LAN Setup' in red. Below the title, there are several configuration fields: 'MAC Address' with the value '00:90:4C:88:88:88', 'IP Address Type' set to 'Dynamic' in a dropdown menu, 'Device Name' set to 'Wireless Access Point' in a text box, and 'Driving Capability of Port' with radio buttons for 'Standard' (selected) and 'Enhanced (lower port speed)'. On the right side, there are three buttons: 'Save', 'Restore', and 'Help'. A mouse cursor is pointing at the 'Save' button.

---End

After the configuration, if you want to log in to the web UI of your AP, first find the IP address of the AP from the client list of the DHCP server, then ensure that the IP address of your computer and the IP address of the AP belong to the same network segment, finally log in to the web UI of your AP using its new IP address.

Note

If the IP address of your computer is not in the same network segment with the new IP address of your AP, please set an IP address for your computer which is in the same network segment as the AP's new IP address. For detailed steps to set an IP address for your computer, refer to **Appendix A** in this user guide.

7.2.2 Static IP address

If you want to set AP's IP address yourself, set **IP Address Type** to **Static** first, then configure IP address, subnet mask, gateway IP address, and DNS server IP addresses for your AP manually. This type is recommended only when you need to deploy just a few APs.

Procedure:

1. To access the configuration page, click **Network > LAN Setup**.
2. Set **IP Address Type** to **Static**.
3. **IP Address:** Enter the static IP address for your AP, which is **192.168.0.250** in this example.

- 4. Subnet Mask:** Enter the subnet mask for your AP, which is **255.255.255.0** in this example.
- 5. Gateway:** Enter the gateway for your AP, which is **192.168.0.1** in this example.
- 6. Primary DNS Server:** Enter the primary DNS server for your AP, which is **8.8.8.8** in this example.
- 7. Secondary DNS Server:** If this parameter is available, enter the secondary DNS server for your AP, which is **8.8.4.4** in this example. Otherwise, leave this box blank.
- 8. Click Save.**

The screenshot shows the 'LAN Setup' configuration page for a wireless access point. The page title is 'LAN Setup' and the user is logged in as 'Administrator:admin'. The configuration fields are as follows:

MAC Address	00:90:4C:88:88:88	
IP Address Type	Static	
IP Address	192.168.0.250	Example: 192.168.1.254
Subnet Mask	255.255.255.0	Example: 255.255.255.0
Gateway	192.168.0.1	
Primary DNS Server	8.8.8.8	
Secondary DNS Server	8.8.4.4	(optional)
Device Name	Wireless Access Point	
Driving Capability of Port	<input checked="" type="radio"/> Standard <input type="radio"/> Enhanced (lower port speed)	

Buttons: Save, Restore, Help

---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.

7.3 DHCP server

7.3.1 Overview

The AP supports the DHCP server function to assign IP addresses to devices connected to it. However, the AP's DHCP server function is disabled by default, so as to make the devices connected to the AP can access the internet successfully.


7.3.2 Configuring the DHCP server



1. To access the configuration page, choose **Network > DHCP Server**.
2. **DHCP Server**: Tick **Enable**.
3. **Gateway**: Enter the gateway address, which is **192.168.0.1** in this example.
4. **Primary DNS Server**: Enter the primary DNS server, which is **8.8.8.8** in this example.
5. Click **Save**.

The screenshot shows the DHCP Server configuration interface. At the top right, it says 'Administrator:admin'. Below that, there are two tabs: 'DHCP Server' (selected) and 'DHCP Clients'. The main area contains several configuration fields: 'DHCP Server' with a checked 'Enable' checkbox; 'Start IP Address' (192.168.0.100); 'End IP Address' (192.168.0.200); 'Lease Time' (1 day); 'Subnet Mask' (255.255.255.0); 'Gateway' (192.168.0.1); 'Primary DNS Server' (8.8.8.8); and 'Secondary DNS Server' (8.8.4.4) with '(optional)' next to it. On the right side, there are three buttons: 'Save', 'Restore', and 'Help'.

---End

Parameter description

Parameter	Description
DHCP Server	It specifies whether 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 192.168.0.100.
End IP Address	It specifies the end IP address of the DHCP server's IP address pool. The default value is 192.168.0.200.
	 Tip
	The start and end IP addresses must belong to the same network segment as the IP

Parameter	Description
	address of the AP.
Lease Time	<p>It specifies the validity period of an IP address assigned by the DHCP server to a device.</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 1 day.</p>
Subnet Mask	It specifies the subnet mask assigned by the DHCP server to devices. The default value is 255.255.255.0.
Gateway	<p>It specifies the gateway IP address assigned by the DHCP server to devices. Generally, it is the LAN IP address of the LAN router connected to the internet. The default value is 192.168.0.1.</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 Server	<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 Server	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.

 **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.

7.3.3 DHCP clients

If the AP's DHCP server function is enabled, this module enables you to view detailed information about devices that obtain IP addresses from the AP's DHCP server, which includes host names, IP addresses, MAC addresses, and lease times.

To access the page, choose **Network > DHCP Server > DHCP Clients**.

Administrator:admin

DHCP Server **DHCP Clients**

If the DHCP server is enabled, the client list is updated every five seconds. Refresh

ID	Host Name	IP Address	MAC Address	Lease Time
1	Tom-PC	192.168.0.129	4c:cc:6a:ad:14:53	23:59:00

If the DHCP server is enabled, your AP will update its client list every five seconds. You can also click **Refresh** to view the latest DHCP client list.

8 Wireless

8.1 Basic

8.1.1 Overview

This module enables you to set SSID-related parameters of the AP. However, you are only recommended to change the SSID, security mode but retain the other default settings. To access the configuration page, click **Wireless > Basic**.

The screenshot shows the configuration interface for the Wireless module, specifically the Basic tab. The left sidebar contains a navigation menu with options: Status, Quick Setup, Network, Wireless, Basic (selected), RF, Radio Optimizing, Illegal AP Detection, WMM Setup, Access Control, Advanced, QVLAN Setup, SNMP, Deployment, and Tools. The main content area is titled 'Basic' and shows the following settings:

Parameter	Value
SSID	IP-COM_WIFI
Enable	<input checked="" type="checkbox"/>
Broadcast SSID	Enable
Isolate Client	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
WMF	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Probe Broadcast Packets Control	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Max. Number of Clients	48 (Range: 1 - 128)
SSID	IP-COM_WIFI
Chinese SSID Encoding	UTF-8
Security Mode	None

Buttons for Save, Restore, and Help are located on the right side of the configuration area. The user is logged in as Administrator:admin.

Broadcast SSID

When the AP broadcasts an SSID, wireless devices nearby can detect the SSID. When this parameter is set to **Disable**, the AP does not broadcast the SSID so that nearby wireless devices cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless devices to connect to the WiFi network corresponding to the SSID. To some extent, disabling broadcasting SSID enhances the security of the WiFi network.

However, even though **Broadcast SSID** is set to **Disable**, a hacker can still connect to the corresponding WiFi network if he/she manages to obtain the SSID by other means.

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 such as hotels and airports to improve network security.

WMF

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.

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.

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.

Max. Number of Clients

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 APs.

Chinese SSID Encoding

It specifies the encoding format of Chinese SSIDs, which consists of UTF-8 (default) and GB2312. This setting is effective only when an SSID contains Chinese characters. If you want your Chinese SSID to be displayed properly, select the encoding format supported by your wireless devices.

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**, **WPA**, and **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 WiFi LAN 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 help increase network security significantly, making WPA and WPA2 the preferred security modes of WiFi networks that require high security.

8.1.2 Changing the basic settings

To change the basic settings of an SSID, perform the following procedure:

1. Choose **Wireless > Basic**.
2. Select the SSID from the **SSID** drop-down list box.
3. Change the parameters as required. Generally, you only need to set the **SSID**, and **Security Mode**, **Key** parameters.
4. Click **Save**.

Administrator:admin

Basic

SSID	<input type="text" value="Tom-WiFi"/>	<input type="button" value="Save"/>
Enable	<input checked="" type="checkbox"/>	<input type="button" value="Restore"/>
Broadcast SSID	<input type="text" value="Enable"/>	<input type="button" value="Help"/>
Isolate Client	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
WMF	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Probe Broadcast Packets Control	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Max. Number of Clients	<input type="text" value="32"/> (Range: 1 - 128)	
SSID	<input type="text" value="Tom-WiFi"/>	
Chinese SSID Encoding	<input type="text" value="UTF-8"/>	
Security Mode	<input type="text" value="WPA2-PSK"/>	
Encryption Algorithm	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP&AES	
Key	<input type="text" value="*****"/>	
Key Update Interval	<input type="text" value="0"/> (Range: 0 or 60 - 99999; 0: not to update)	

---End

Parameter description

Parameter	Description
SSID	<p>It specifies the SSID to be configured.</p> <p>The AP supports four SSIDs and the first SSID displayed is the primary SSID.</p>
Enable	<p>It specifies whether to enable the selected SSID.</p> <p>The AP supports four SSIDs being enabled concurrently, and the primary SSID is enabled by default, while the other are disabled. Users can enable them if required.</p>
Broadcast SSID	<p>It specifies whether to broadcast the selected SSID.</p> <ul style="list-style-type: none"> – Enable: It indicates that the AP broadcasts the selected SSID. In this case, nearby wireless devices can detect the SSID. – Disable: It indicates that the AP does not broadcast the selected SSID so that nearby wireless devices cannot detect the SSID. In this case, if you want to connect a wireless device to the WiFi network corresponding to the SSID, you must enter the SSID on the device manually.



Tip This AP can hide its SSID automatically. When the number of devices connected to the AP to an SSID of the AP reaches the upper limit, the AP stops broadcasting the SSID.

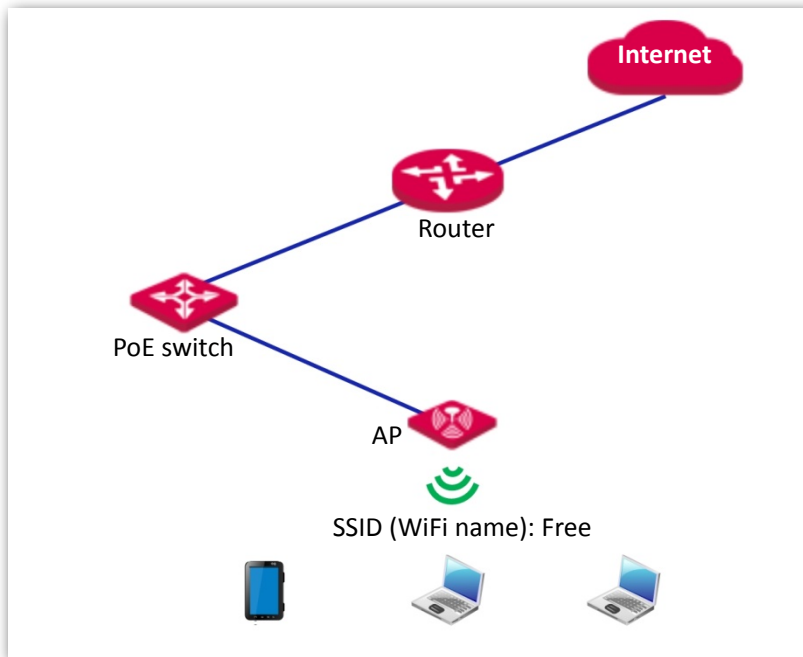
Parameter	Description
Isolate Client	<ul style="list-style-type: none">- Enable: It indicates that the wireless devices connected to the AP with the selected SSID cannot communicate with each other, which improves WiFi network security.- Disable: It indicates that the wireless devices connected to the AP with the selected SSID can communicate with each other. By default, Isolate Client is disabled.
WMF	<ul style="list-style-type: none">- Enable: It indicates that the WMF function is enabled.- Disable: It indicates that the WMF function is disabled. By default, WMF function is disabled.
Probe Broadcast Packets Control	<ul style="list-style-type: none">- Enable: It indicates that the Probe Broadcast Packets Control function is enabled.- Disable: It indicates that the Probe Broadcast Packets Control function is disabled. By default, the function is disabled.
Max. Number of Clients	<p>It specifies the maximum number of devices that can be concurrently connected to the WiFi network corresponding to an SSID.</p> <p>After this upper limit is reached, the AP rejects new requests from devices for connecting to the wireless network.</p> <p>A maximum of 128 wireless devices are allowed to connect to the enabled SSIDs of the AP.</p>
SSID	If you want to change the selected SSID, enter the new SSID in this box.
Chinese SSID Encoding	It specifies the encoding format of Chinese characters in an SSID. The default value is UTF-8 . This parameter takes effect only if the SSID contains Chinese characters.
Security Mode	It specifies the security mode of the selected SSID. The options include: None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA and WPA2. If you want to change the security mode of the selected SSID, click the drop-down list box and select your desired mode from it.

8.1.3 Examples

Setting up a non-encrypted WiFi network

Networking requirement

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



Procedures:

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

1. Choose **Wireless > Basic**.
2. Select the second SSID from the **SSID** drop-down list box, which is **IP-COM_888889** in this example.
3. Tick the **Enable** box.
4. Set the value of the **SSID** box to **Free**.
5. **Security Mode**: Select **None**.
6. Click **Save**.

Basic Administrator:admin

SSID: IP-COM_888889

Enable:

Broadcast SSID: Enable

Isolate Client: Disable Enable

WMF: Disable Enable

Probe Broadcast Packets Control: Disable Enable

Max. Number of Clients: 32 (Range: 1 - 128)

SSID: Free

Chinese SSID Encoding: UTF-8

Security Mode: None

Save Restore Help

---End

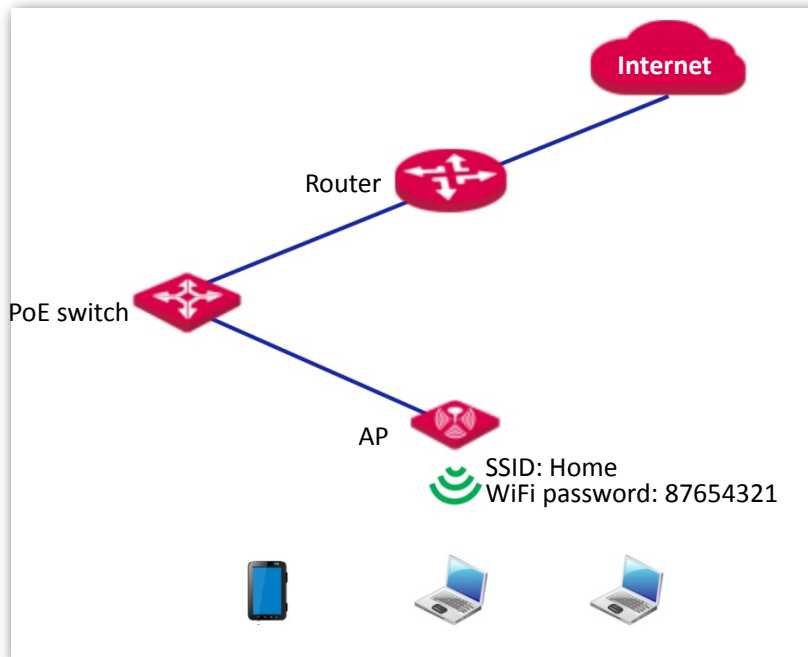
Verification

Wireless devices can connect to the WiFi network named **Free** without a password.

Setting up a WiFi network encrypted by WPA-PSK or WPA2-PSK

Networking requirement

WiFi network at home with a certain level of security must be configured through a simple procedure. In this case, WPA-PSK or WPA2-PSK mode is recommended. See the following figure.



Procedures:

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

1. Choose **Wireless > Basic**.
2. Select the second SSID from the **SSID** drop-down list box, which is **IP-COM_888889** in this example.
3. Tick the **Enable** box.
4. Set the value of the **SSID** box to **Home**.
5. **Security Mode**: Select **WPA2-PSK**.
6. **Encryption Algorithm**: Select **AES**.
7. **Key**: Enter **87654321**.
8. Click **Save**.

The screenshot shows the 'Basic' configuration page for a wireless access point. The page is titled 'Administrator:admin' in the top right corner. The 'Save' button is highlighted with a mouse cursor. The configuration options are as follows:

Field	Value
SSID	IP-COM_888889
Enable	<input checked="" type="checkbox"/>
Broadcast SSID	Enable
Isolate Client	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
WMF	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Probe Broadcast Packets Control	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Max. Number of Clients	32 (Range: 1 - 128)
SSID	Home
Chinese SSID Encoding	UTF-8
Security Mode	WPA2-PSK
Encryption Algorithm	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP&AES
Key	*****
Key Update Interval	0 (Range: 0 or 60 - 99999; 0: not to update)

---End

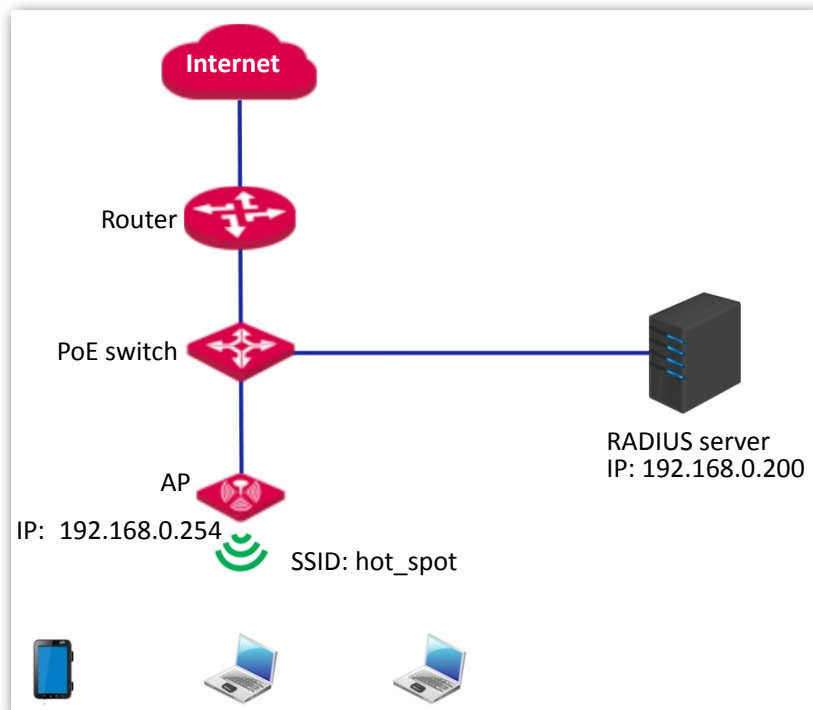
Verification

Wireless devices can connect to the WiFi network named **Home** using the password 87654321.

Setting up a WiFi network encrypted by WPA or WPA2

Networking requirement

In this case a highly secure WiFi network is required and a RADIUS server is available. To fulfill the requirement, WPA or WPA2 mode is recommended. See the following figure.



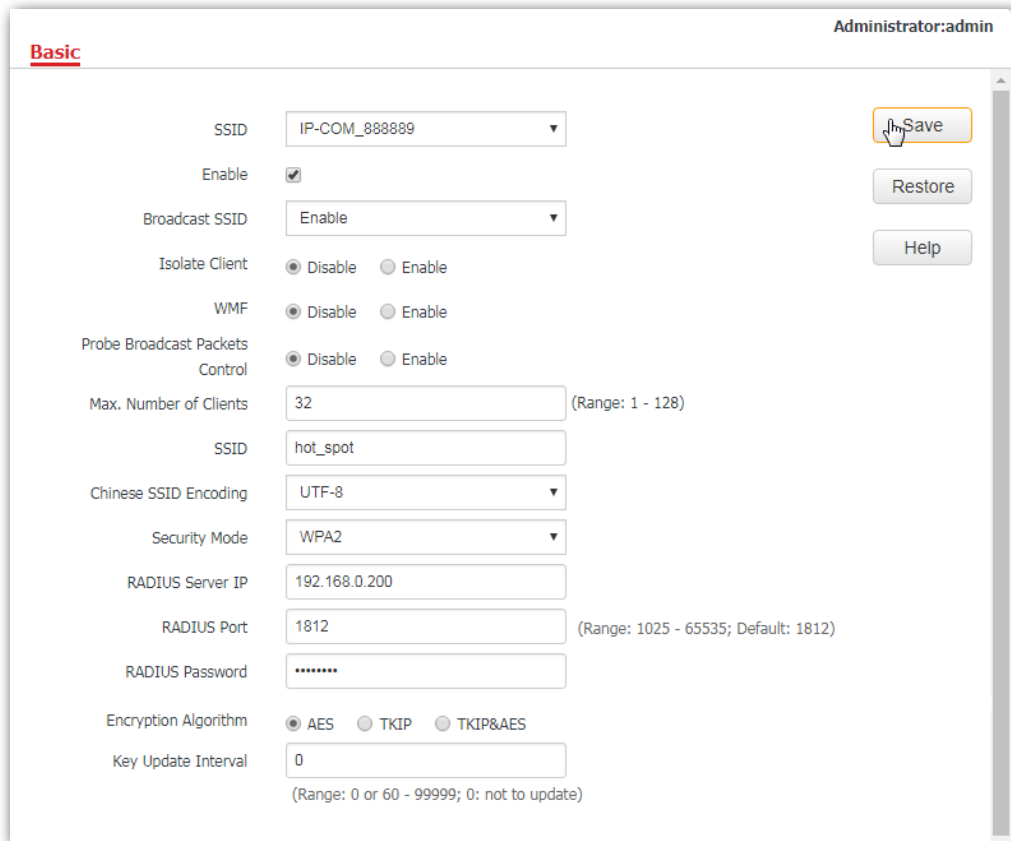
Procedures:

1. Configure the AP.

Assume that the IP address of the RADIUS server is 192.168.0.200, the password is 12345678, and the port number for authentication is 1812.

Assume that the second SSID of the AP is used.

- (1) Choose Wireless > Basic.
- (2) Select the second SSID from the **SSID** drop-down list box.
- (3) Tick the **Enable** box.
- (4) Change the value of the **SSID** text box to **hot_spot**.
- (5) Set **Security Mode** to **WPA2**.
- (6) Set **RADIUS Server IP**, **RADIUS Port**, and **RADIUS Password** to **192.168.0.200**, **1812**, and **12345678** respectively.
- (7) **Encryption Algorithm**: Select **AES**.
- (8) Click **Save**.



2. Configure the RADIUS server.

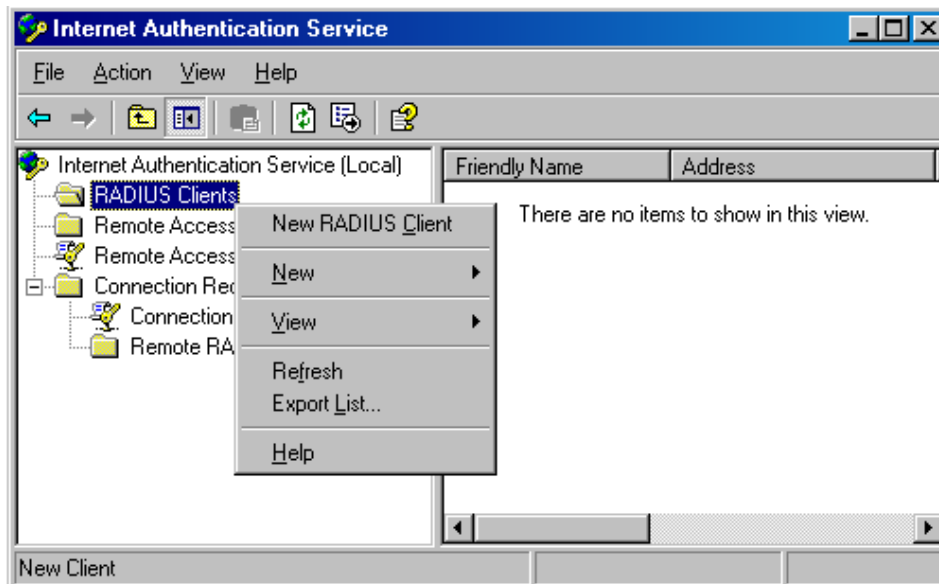


Note

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

(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 (which can be the name of the AP) and the IP address of the AP, and

click **Next**.

New RADIUS Client

Name and Address

Type a friendly name and either an IP Address or DNS name for the client.

Friendly name:

Client address (IP or DNS):

IP address of the AP

< Back Next > Cancel

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

New RADIUS Client

Additional Information

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

Client-Vendor:

Shared secret:

Confirm shared secret:

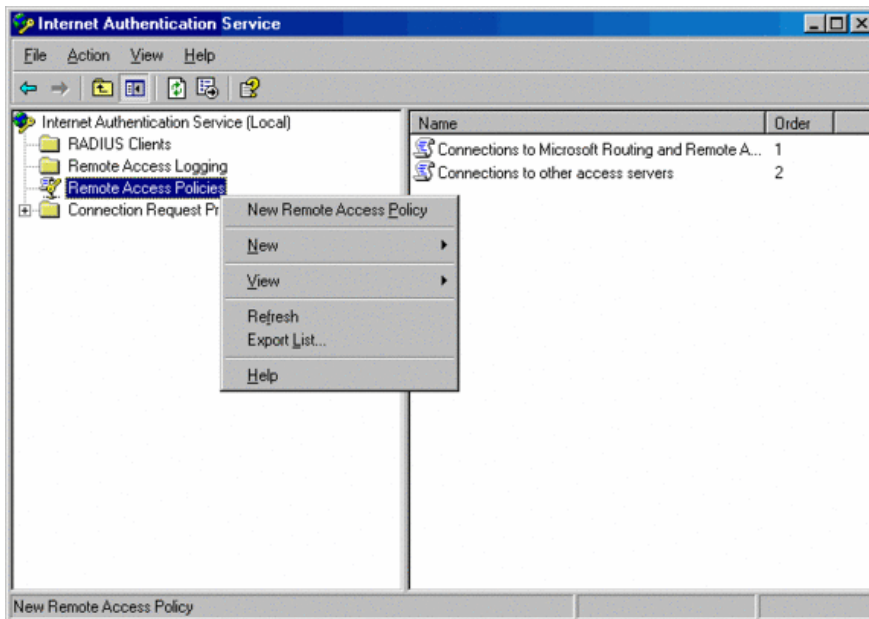
Request must contain the Message Authenticator attribute

Password same as that specified by RADIUS Password on the AP.

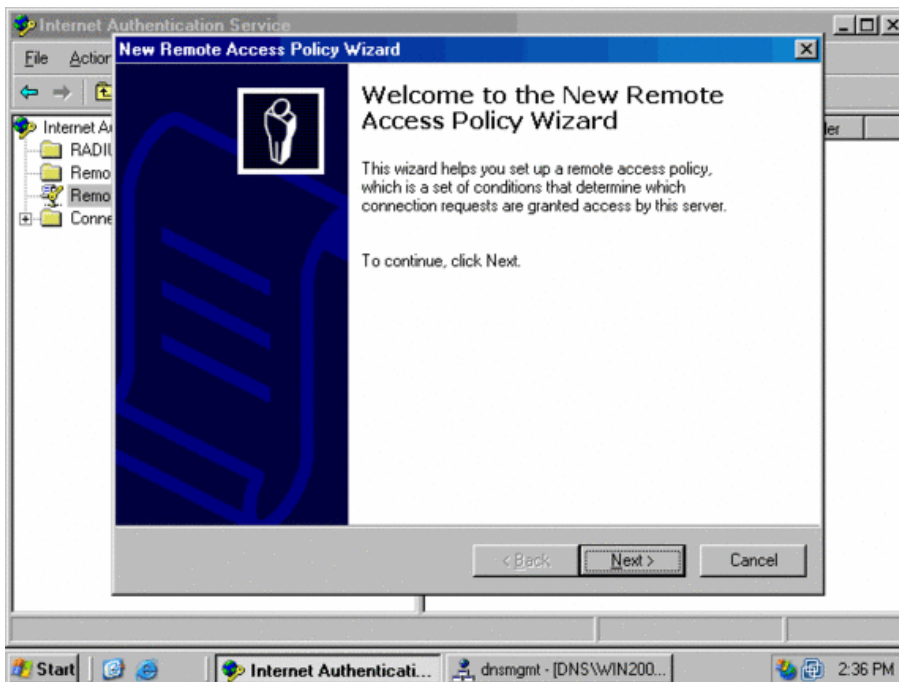
< Back Finish Cancel

- (2) Configure a remote access policy.

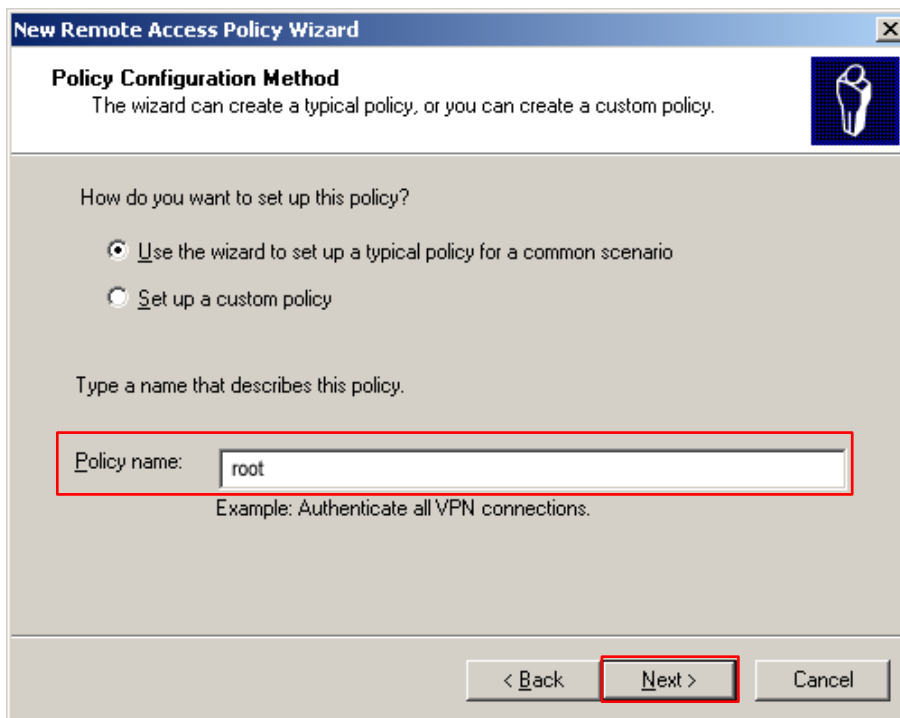
Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



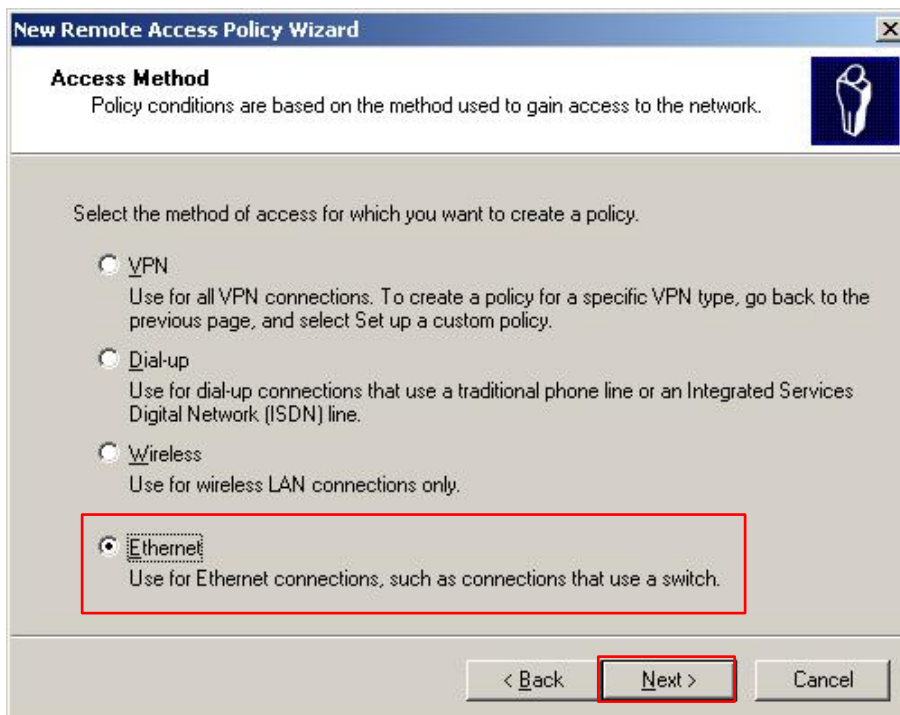
In the **New Remote Access Policy Wizard** dialog box that appears, click **Next**.



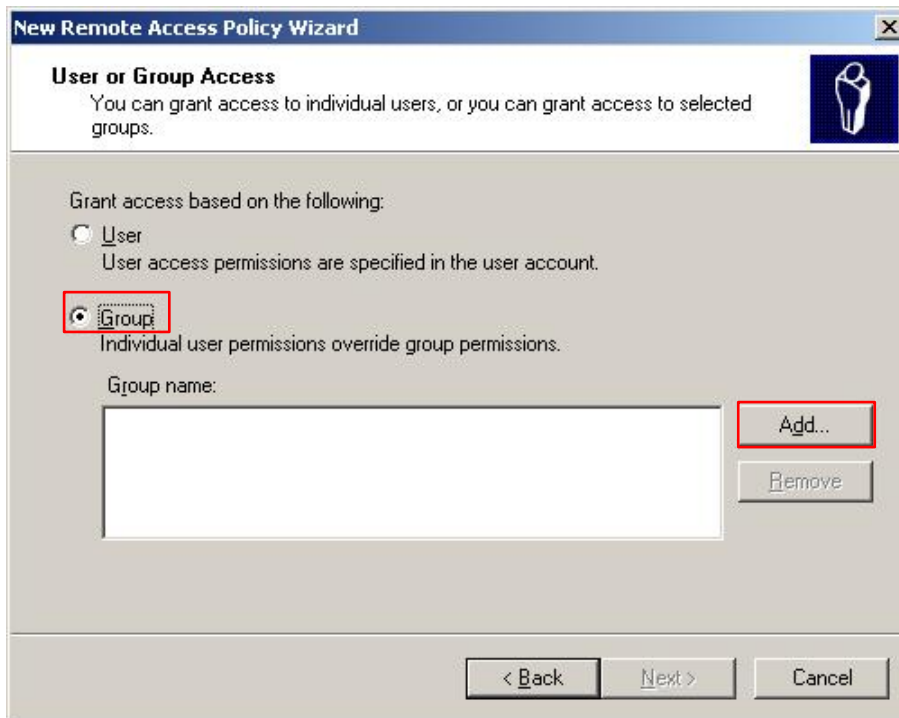
Enter a policy name and click **Next**.



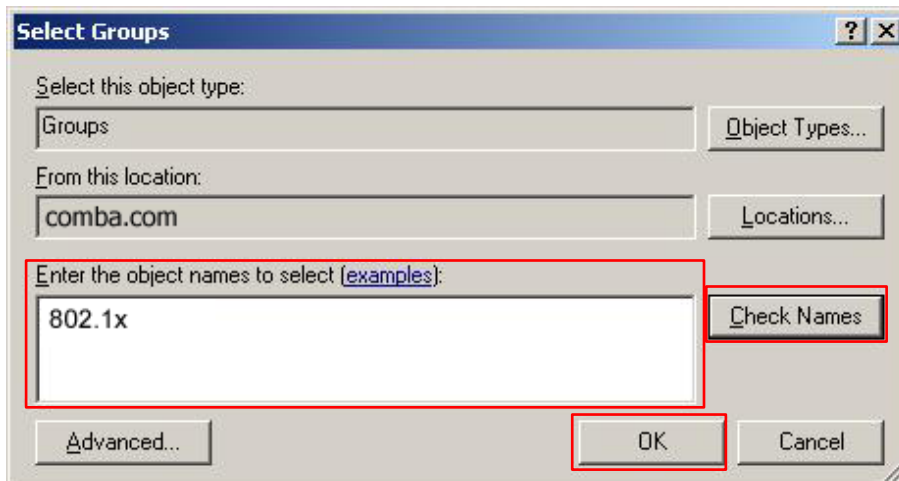
Select **Ethernet** and click **Next**.



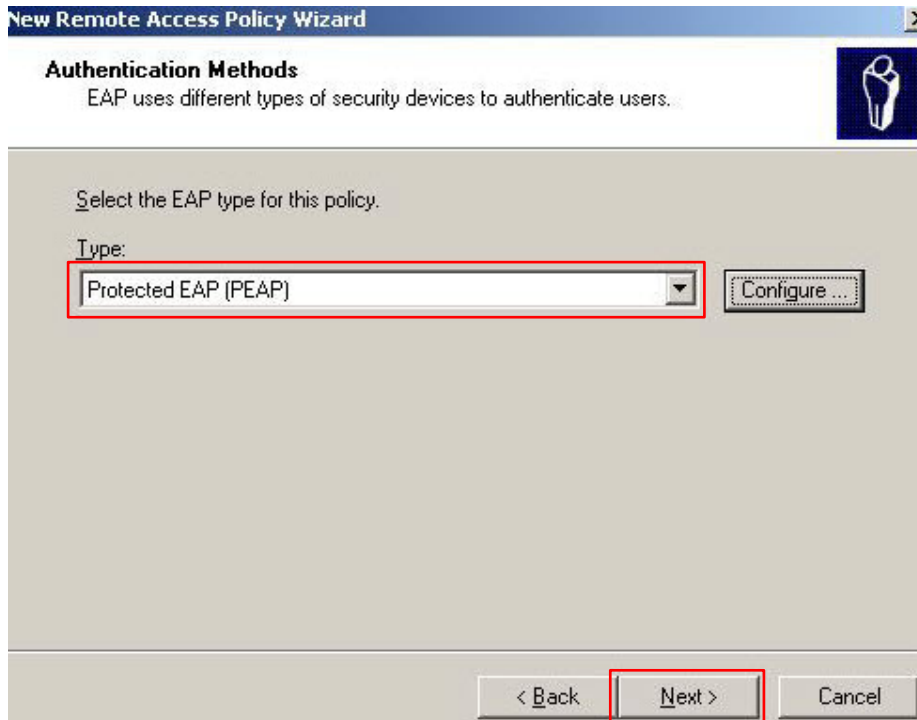
Select **Group** and click **Add**.



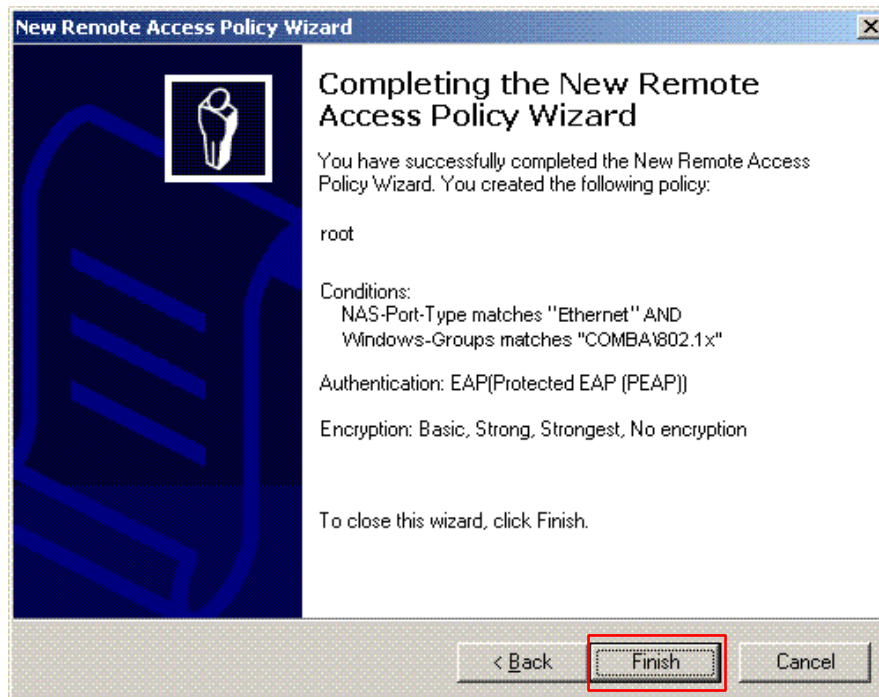
Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



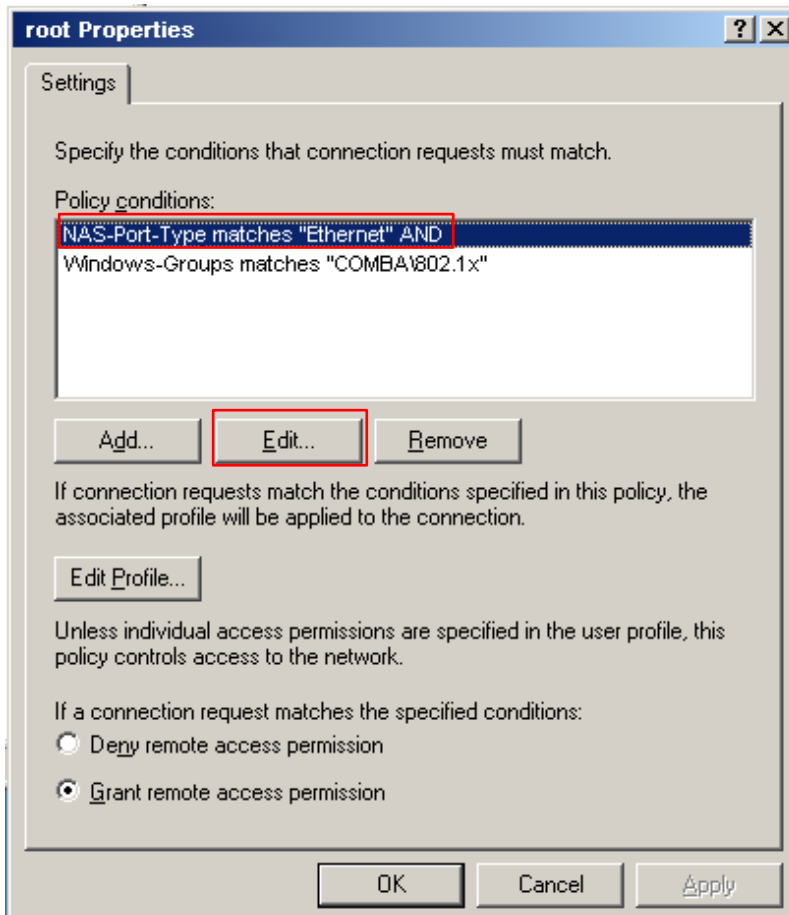
Select **Protected EAP (PEAP)** and click **Next**.



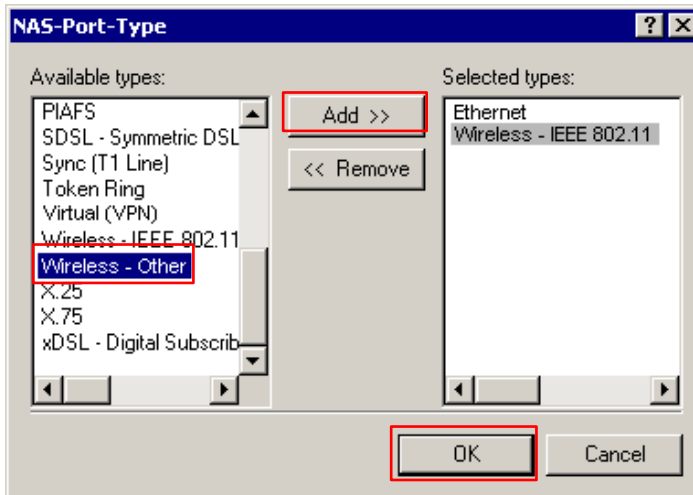
Click **Finish**. The remote access policy is created.



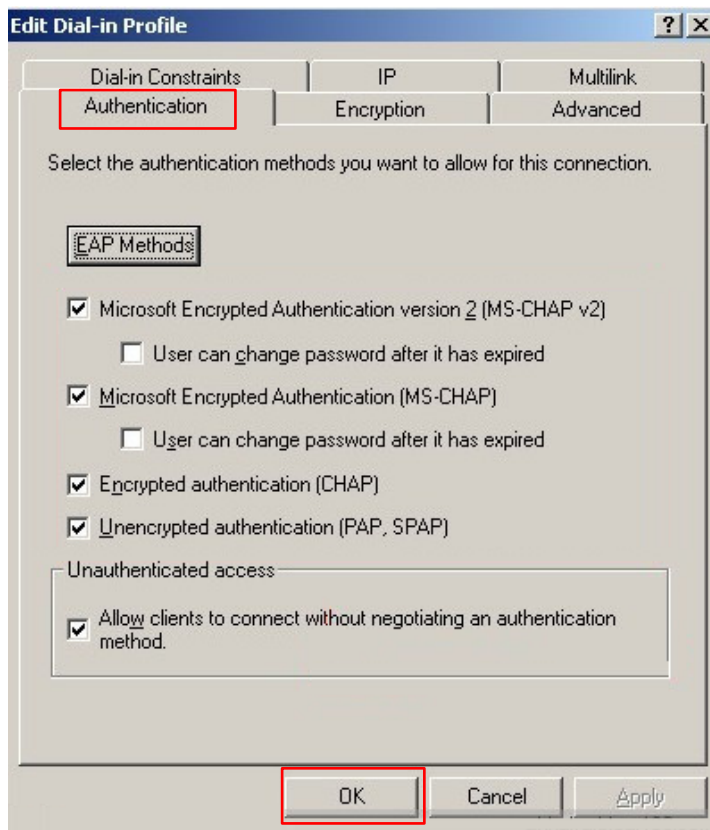
Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



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



Click **Edit 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

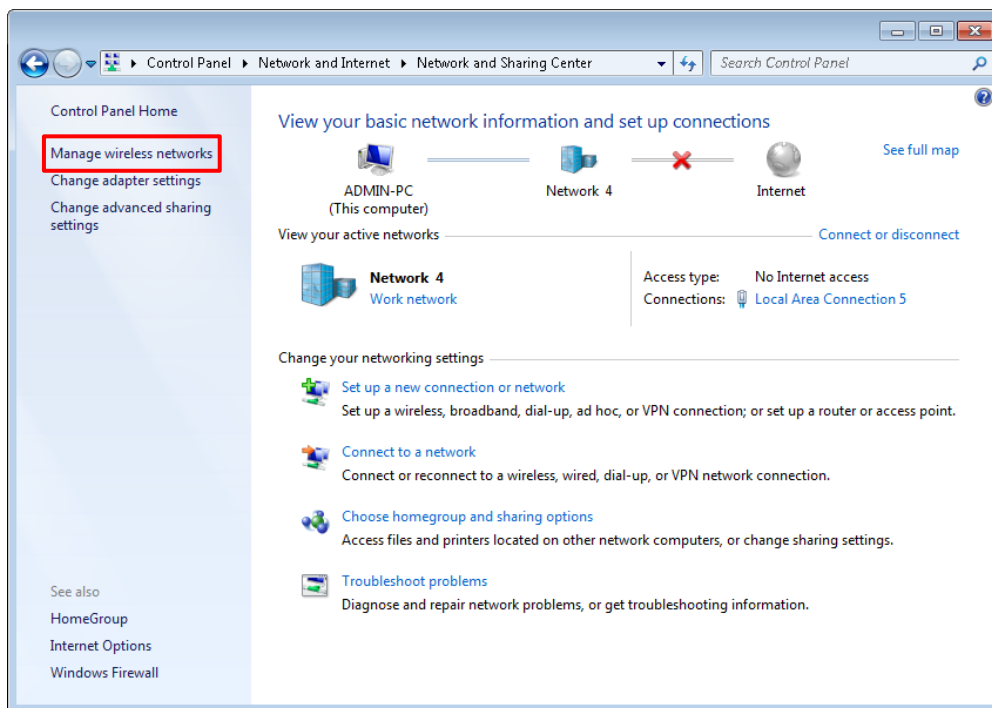
Configure your wireless device.



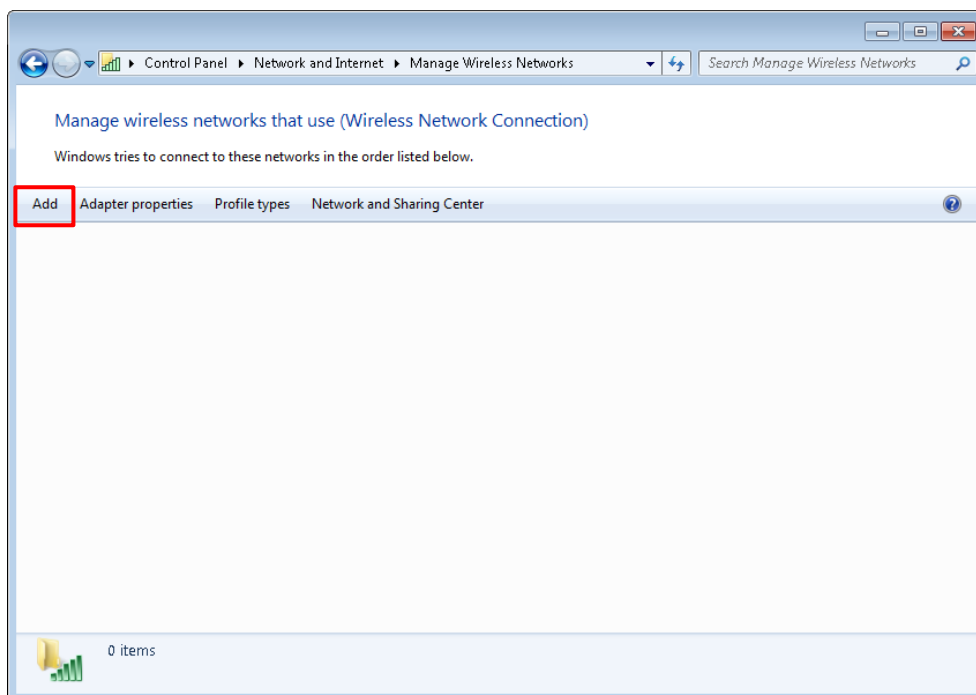
Tip

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

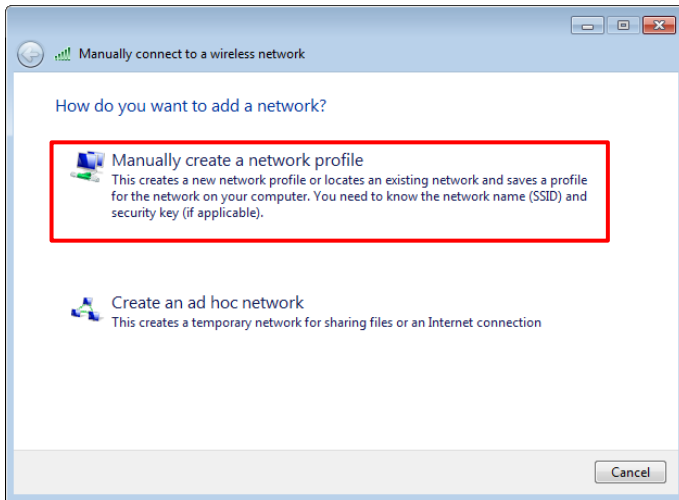
Choose **Start > Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



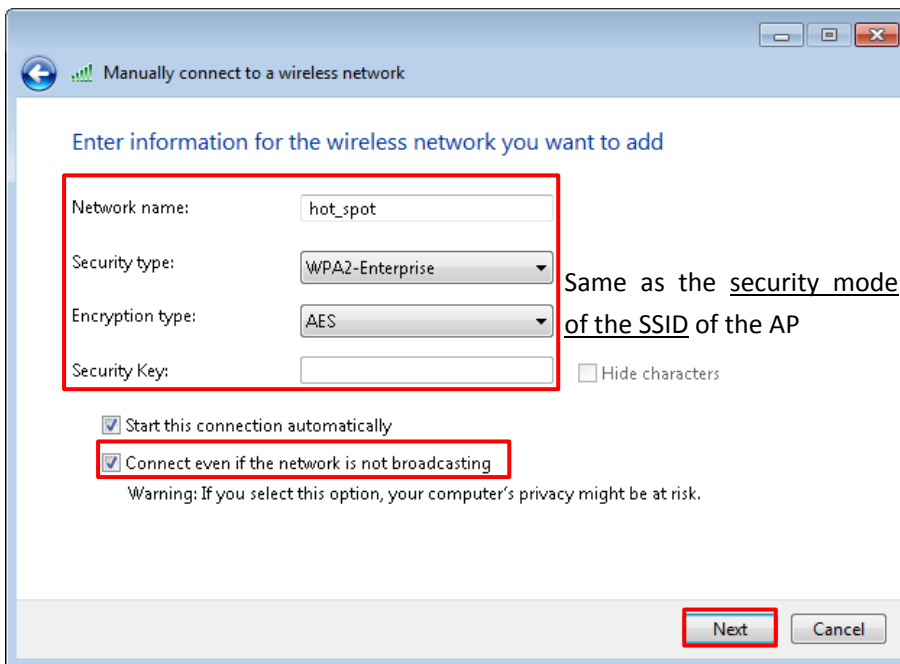
Click **Add**.



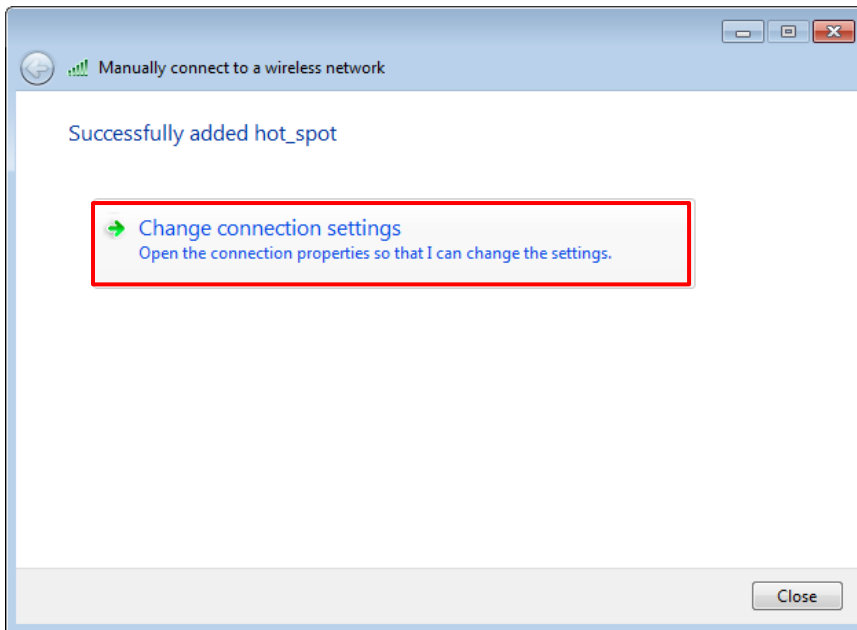
Click **Manually create a network profile**.



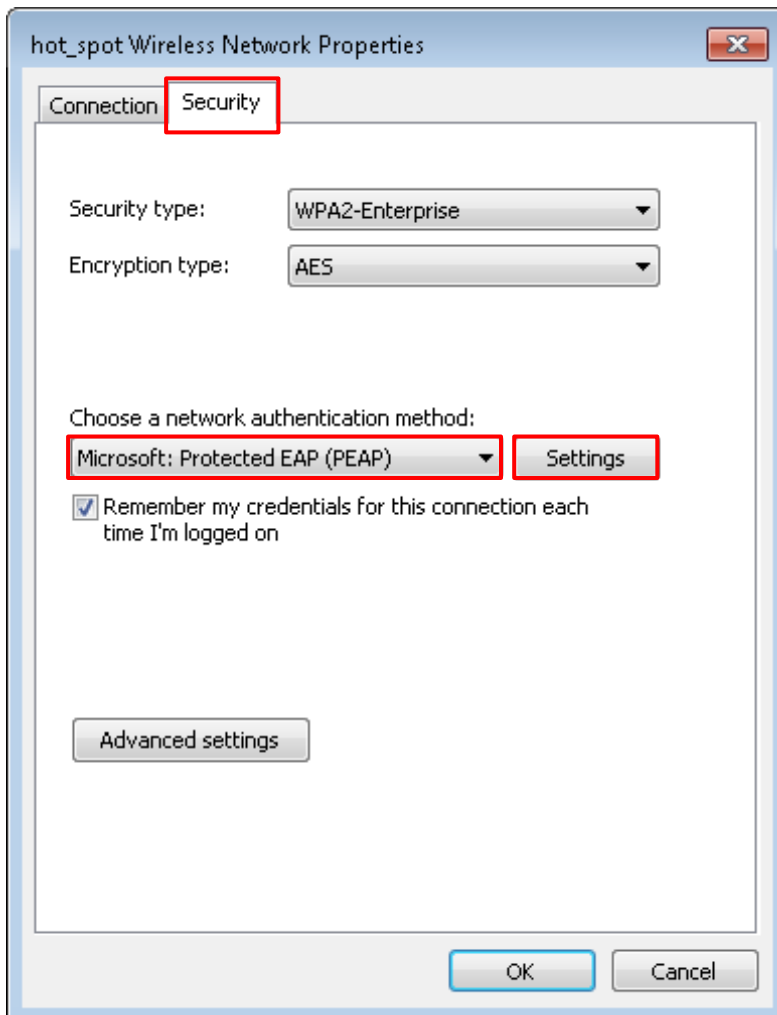
Enter WiFi network information, select **Connect even if the network is not broadcasting**, and click **Next**.



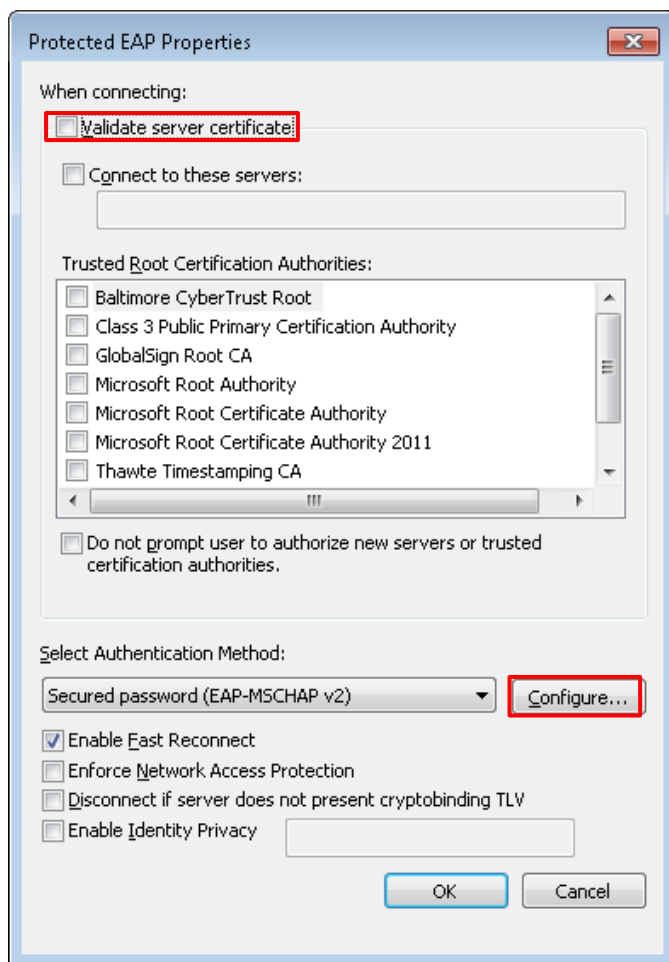
Click **Change connection settings**.



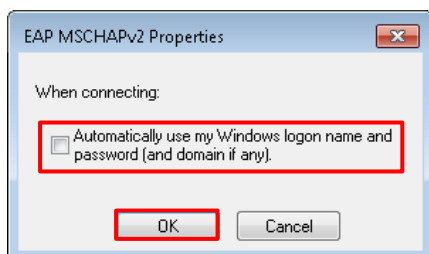
Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



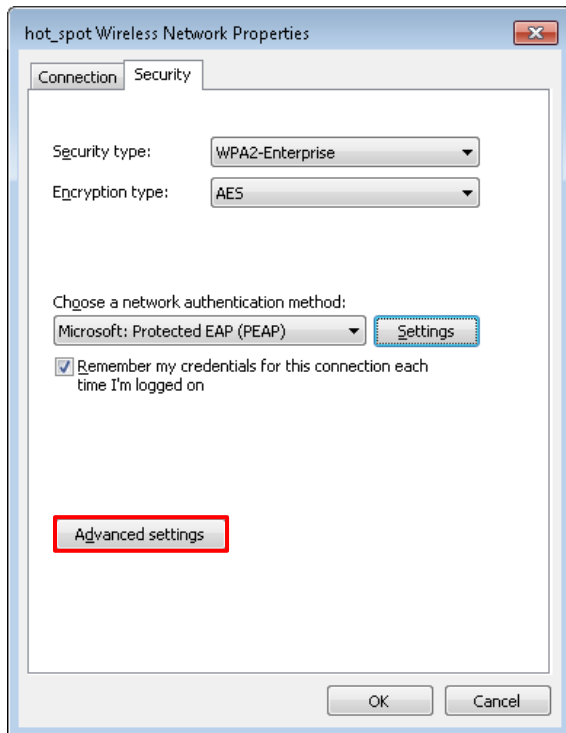
Deselect **Validate server certificate** and click **Configure**.



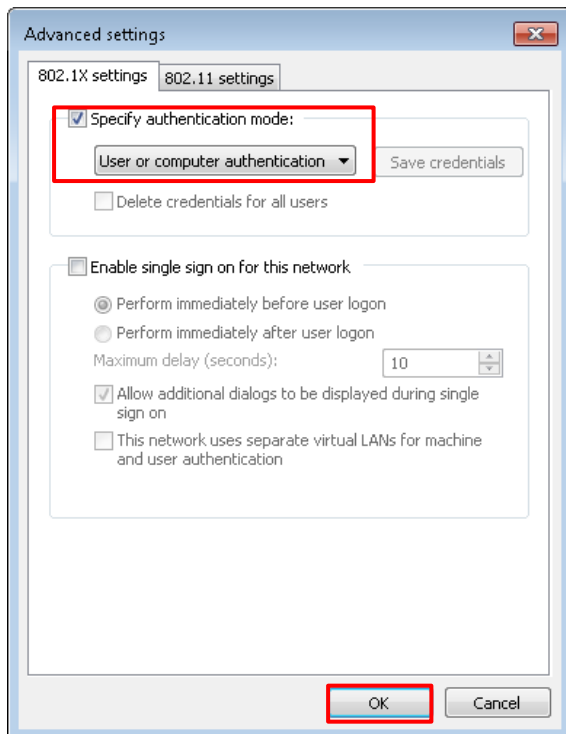
Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



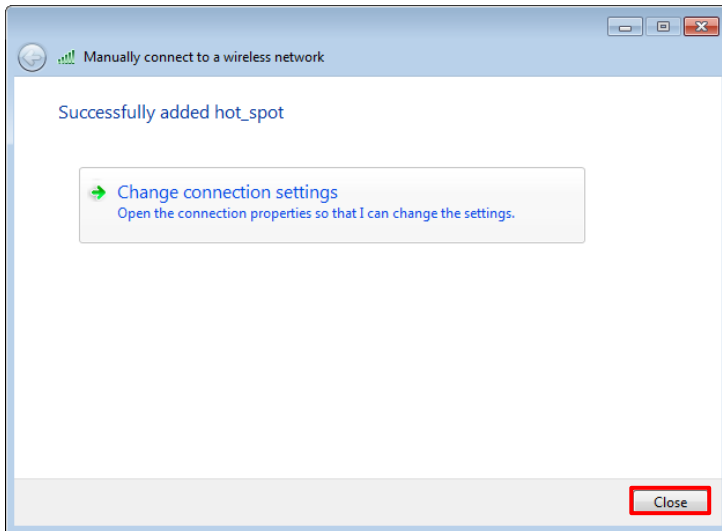
Click **Advanced settings**.



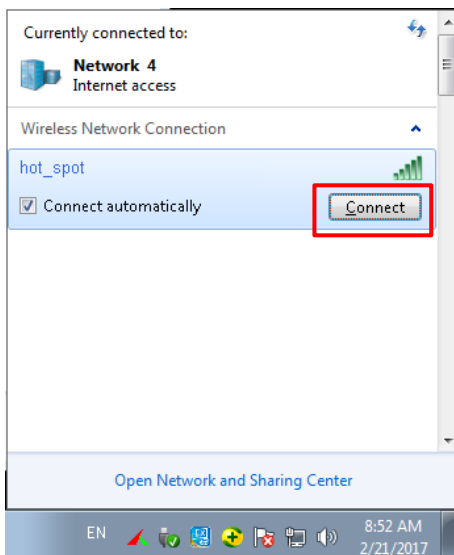
Tick **User or computer authentication** and click **OK**.



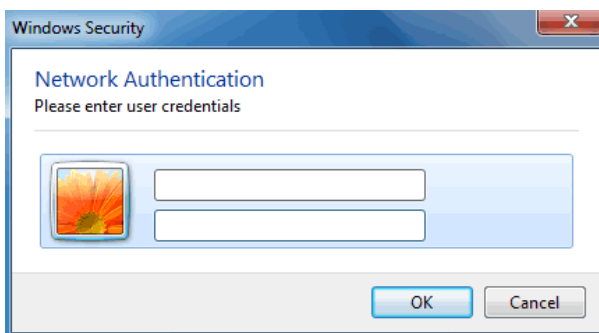
Click **Close**.



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**.



Verification

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

8.2 RF

8.2.1 Overview

The RF module is used to set radio parameters of the AP, such as country/region and network mode. It also enables you to turn on/off the Isolate SSID function. The following describes the Isolate SSID function briefly.

Isolate SSID

This function isolates the wireless devices connected to different WiFi networks of the AP. For example, if user A connects to the WiFi network corresponding to SSID1, whereas user B connects to the WiFi network corresponding to SSID2, the two users cannot communicate with each other after Isolate SSID is enabled.



8.2.2 Changing the RF settings

1. Choose **Wireless > RF**.
2. Change the parameters as required. Generally, you only need to change the **Enable RF**, **Channel**, and **Lock Channel** settings.
3. Click **Save**.

---End

Parameter description

Parameter	Description
Enable RF	It specifies whether to enable the radio function of the AP.
Country/Region	It specifies the country or region where the AP is used. This parameter helps comply with channel regulations of the country or region. The default value is China .
Network Mode	It specifies the WiFi network mode of the AP, which includes 11b, 11g, 11b/g, and 11b/g/n. This parameter can be set if Lock Channel is not selected. <ul style="list-style-type: none"> – 11b: The AP works in 802.11b mode and only wireless devices compliant with 802.11b can connect to the WiFi networks of the AP. – 11g: The AP works in 802.11g mode and only wireless devices compliant with 802.11g can connect to the WiFi networks of the AP. – 11b/g: The AP works in 802.11b/g mode and only wireless devices compliant with 802.11b or 802.11g can connect to the WiFi networks of the AP. – 11b/g/n: The AP works in 802.11b/g/n mode. Wireless devices can connect to the WiFi networks of the AP if they are compliant with 802.11b or 802.11g, or they work at 2.4 GHz and compliant with 802.11n.
Channel	It specifies the operating channel of the AP. This parameter can be set if Lock Channel is not selected. If you select Auto from the drop-down-list box, the AP adjusts its operating channel automatically according to the ambient environment.
Channel Bandwidth	It specifies the wireless channel bandwidth of the AP. This parameter can be set if the AP works in 802.11 b/g/n mode and Lock Channel is not selected. <ul style="list-style-type: none"> – 20: It indicates that the AP can use only 20 MHz channel bandwidth. – 40: It indicates that the AP uses 40 MHz channel bandwidth first, and changes to 20 MHz channel bandwidth if severe channel competition occurs in the ambient environment.

Parameter	Description
	<ul style="list-style-type: none">– 20/40: It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment.
Extension Channel	It specifies the wireless extension channel of the AP.
Lock Channel	It is used to lock the channel settings of the AP. If this parameter is selected, channel settings including Country/Region, Network Mode, Channel, Channel Bandwidth, and Extension Channel cannot be changed.
Transmit Power	It specifies the transmit power of the AP. The default value is 8 dBm. If the AP has a higher transmit power, its WiFi coverage is wider. However, reasonably decreasing the transmit power will improve the AP's WiFi network performance and security.
Lock Power	It specifies whether the current transmit power settings of the AP can be changed. If you tick this box, the current transmit power could not be changed.
Preamble	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. By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless devices. To achieve better synchronization performance of networks, you can select the Short Preamble option.
Isolate SSID	It specifies whether to isolate the wireless devices connected to the AP with different SSIDs. <ul style="list-style-type: none">– Disable: It specifies the Isolate SSID function is disabled, so that the wireless devices connected to the AP with different SSIDs can communicate with each other.– Enable: It specifies the Isolate SSID function is enabled, so that the wireless devices connected to the AP with different SSID cannot communicate with each other, which improves WiFi network security.
Short GI	It specifies short guard interval. Propagation delay of WiFi signal will happen to the receiving port during transmission. If the following data block is sent too fast, it will interfere the previous data block. A short guard interval can be used to circumvent this interference. Enabling the short GI function can yield a 10% improvement in data throughput. By default, this function is enabled.

8.3 Radio Optimizing

8.3.1 Changing the radio optimizing settings



It is recommended to change the settings only under the instruction of professional personnel, so as to prevent wireless performance from getting worse.

1. Choose **Wireless > Radio Optimizing**.
2. Change the parameter settings as required.
3. Click **Save**.

Radio Optimizing Administrator:admin

Beacon Interval: 100 ms (Range: 100 - 999; Default: 100)

Fragment Threshold: 2346 (Range: 256 - 2346; Default: 2346)

RTS Threshold: 2347 (Range: 1 - 2347; Default: 2347)

DTIM Interval: 1 (Range: 1 - 255; Default: 1)

Min. RSSI Threshold: Enable Disable -90 dBm (Range: -99 - -60; Default: -90)

Interference Mitigation: 2 (Range: 0 - 3; Default: 2)

APSD: Enable Disable

Client Timeout Interval: 5 minutes

Basic Rate Sets: 1 2 5.5 6 9 11 12 18 24 36 48 54 All

Supported Rate Sets: 1 2 5.5 6 9 11 12 18 24 36 48 54 All

Buttons: Save, Restore, Help

---End

Parameter description

Parameter	Description
Beacon Interval	<p>It specifies the interval for transmitting the Beacon frame. The value range is 100 to 999, with a unit millisecond.</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>
Fragment Threshold	<p>It specifies the threshold of a fragment. The value range is 256 to 2346, with a unit byte.</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</p>

Parameter	Description
	<p>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.</p> <p>If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The value range is 1 to 2347, with a unit byte.</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>
DTIM Interval	<p>It specifies the interval for transmitting the Delivery Traffic Indication Message (DTIM) frame. The value range is 1 to 255, with a unit Beacon.</p> <p>A countdown starts from this value. The AP transmits broadcast and multicast frames in its cache only when the countdown reaches zero.</p> <p>For example, if DTIM Interval is set to 1, the AP transmits all cached frames after each beacon frame is transmitted.</p>
Min. RSSI Threshold	<p>It specifies whether to enable the Min. RSSI Threshold function. After you enabled this function, a minimum strength of received signals acceptable to the AP should be set. 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 Min. RSSI Threshold ensures that wireless devices can connect to the AP' WiFi networks with strong signals.</p>
Interference Mitigation	<p>Select an interference mitigation mode for your AP.</p> <ul style="list-style-type: none">– 0: The energy detection mechanism is disabled.– 1: The energy detection mechanism is enabled. When the received signal strength is weaker than -70 dBm, this device stops transmitting data, so as to prevent packet loss due to interference.– 2: The energy detection mechanism is enabled. When the received signal strength is weaker than -50 dBm, this device stops transmitting data, so as to prevent packet loss due to interference.– 3: The energy detection mechanism is enabled. When the received signal strength is weaker than -70 dBm, this device automatically switches to a better channel.
APSD	<p>It enables the AP to reduce power consumption after a specified period during which no traffic is transmitted or received by the AP. By default, it is disabled.</p>
Client Timeout Interval	<p>It specifies the wireless device disconnection interval of the AP. The AP disconnects a wireless device if no traffic is transmitted or received by the wireless client within the interval.</p>
Basic Rate Sets	<p>Select the transmission rate sets you want the AP to support. Wireless devices must supports the basic rate sets you select, or they cannot connect to the AP's WiFi networks.</p>
Supported Rate Sets	<p>Select the transmission rate sets you want the AP to support. Unlike the basic rate sets, it is acceptable for wireless devices not to support the supported rate sets you select.</p>

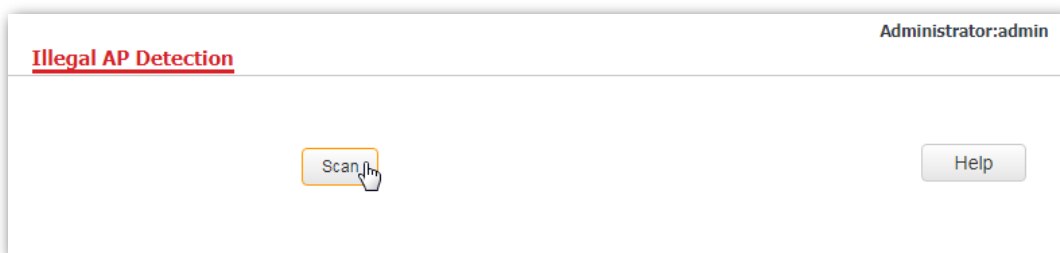
8.4 Illegal AP Detection

8.4.1 Overview

This function enables you to learn about the wireless signals near the AP, including information about SSID, MAC address, channel, and signal strength.

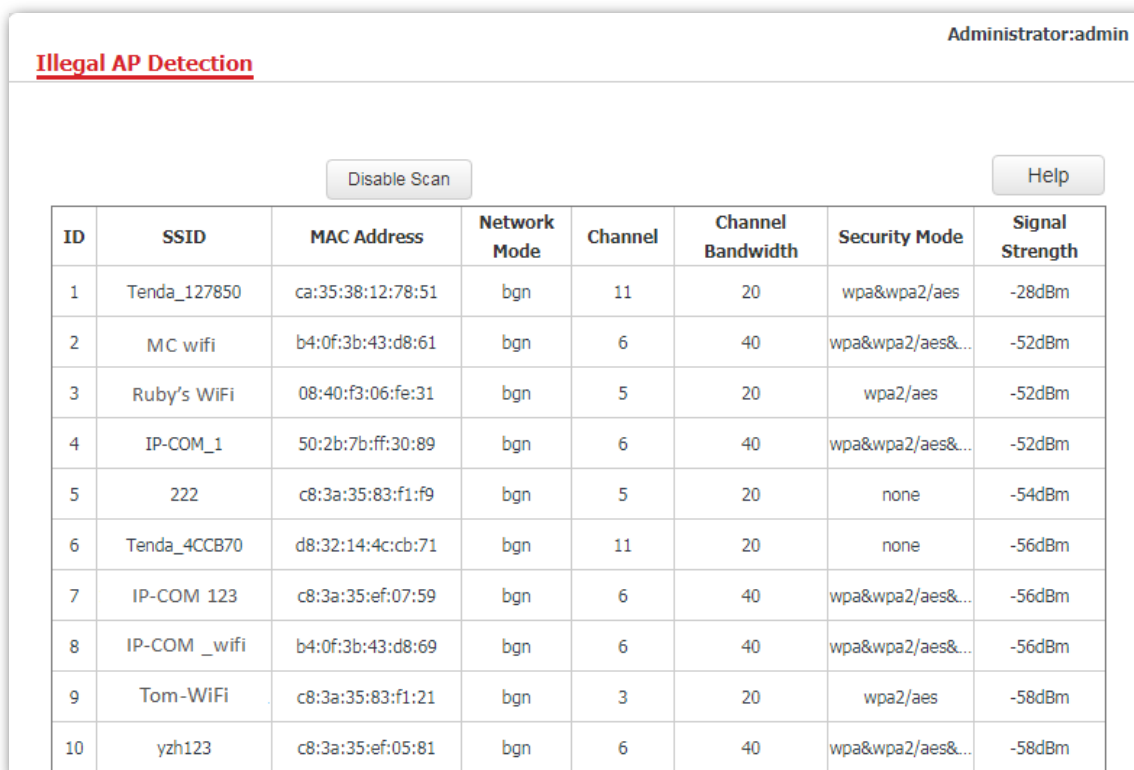
8.4.2 Scanning wireless signals nearby

1. Choose **Wireless > Illegal AP Detection**.
2. Click **Scan**.



---End

The following picture displays the scanning results.



The screenshot shows the 'Illegal AP Detection' interface after a scan. At the top right, it says 'Administrator:admin'. The page title is 'Illegal AP Detection'. In the center, there is a 'Disable Scan' button. To the right of the 'Disable Scan' button is a 'Help' button. Below the buttons is a table with 8 columns: ID, SSID, MAC Address, Network Mode, Channel, Channel Bandwidth, Security Mode, and Signal Strength. The table contains 10 rows of scanning results.

ID	SSID	MAC Address	Network Mode	Channel	Channel Bandwidth	Security Mode	Signal Strength
1	Tenda_127850	ca:35:38:12:78:51	bgn	11	20	wpa&wpa2/aes	-28dBm
2	MC wifi	b4:0f:3b:43:d8:61	bgn	6	40	wpa&wpa2/aes&...	-52dBm
3	Ruby's WiFi	08:40:f3:06:fe:31	bgn	5	20	wpa2/aes	-52dBm
4	IP-COM_1	50:2b:7b:ff:30:89	bgn	6	40	wpa&wpa2/aes&...	-52dBm
5	222	c8:3a:35:83:f1:f9	bgn	5	20	none	-54dBm
6	Tenda_4CCB70	d8:32:14:4c:cb:71	bgn	11	20	none	-56dBm
7	IP-COM 123	c8:3a:35:ef:07:59	bgn	6	40	wpa&wpa2/aes&...	-56dBm
8	IP-COM _wifi	b4:0f:3b:43:d8:69	bgn	6	40	wpa&wpa2/aes&...	-56dBm
9	Tom-WiFi	c8:3a:35:83:f1:21	bgn	3	20	wpa2/aes	-58dBm
10	yzh123	c8:3a:35:ef:05:81	bgn	6	40	wpa&wpa2/aes&...	-58dBm

8.5 WMM Setup

8.5.1 Overview

802.11 networks offer wireless access services based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) channel competition mechanism, which allows all wireless 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 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.

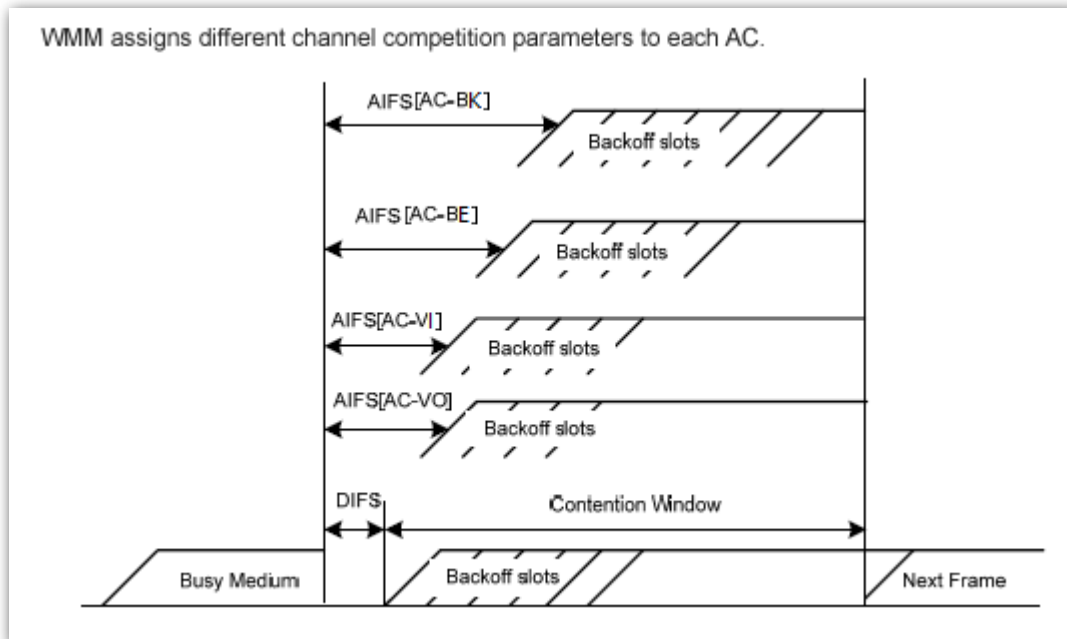
According to the 802.11 protocol family, all devices listen on a channel before using the channel to send data. If the channel stays idle for or longer than a specified period, the devices wait a random backoff period within the contention window. The device whose backoff period expires first can use 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.

■ EDCA Parameters

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

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

- Arbitration Inter Frame Spacing Number (AIFSN): Different from the fixed distributed inter-frame spacing (DIFS) specified in the 802.11 protocol family, AIFSN varies across ACs. A greater AIFSN indicates a longer backoff period. See AIFS in the following figure.
- Contention window minimum (CW_{min}) and contention window maximum (CW_{max}) specify the average backoff period. The period increases along with these two values. See the backoff slots in the following figure.
- Transmission Opportunity (TXOP): It specifies the maximum channel use duration after successful channel contention. The duration increases along with this value. The value **0** indicates that a device can send only one packet through a channel after winning contention for the channel.



■ ACK Policies

WMM specifies the Normal ACK and No ACK policies.

- According to the No ACK policy, no ACK packet is used during wireless packet transmission to acknowledge packet reception. This policy is applicable to scenarios where interference is mild and can effectively improve transmission efficiency. In case of strong interference, lost packets 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.

8.5.2 Changing the WMM Settings

By default, the WMM function of the AP is enabled and the **Optimized For Capacity** mode is adopted. The following procedures describe how to set the WMM settings:

1. Choose **Wireless > WMM Setup**.
2. Set **WMM** to **Enable**.
3. **WMM Optimization Mode**: Select the required WMM optimization mode. If you select **Custom**, set the WMM parameters as required.
4. Click **Save**.

Administrator:admin

2.4GHz WMM

WMM Disable Enable Save

WMM Optimization Mode Optimized For Throughput(Concurrent Users <=10) Restore

Optimized For Capacity(Concurrent Users >=10)

Custom Help

No ACK

EDCA AP Parameters

	CWmin	CWmax	AIFSN	TXOP Limit(usec)
AC_BE	7	63	1	4096
AC_BK	15	1023	7	0
AC_VI	7	15	1	6016
AC_VO	3	7	1	3264

EDCA STA Parameters

	CWmin	CWmax	AIFSN	TXOP Limit(usec)
AC_BE	31	255	2	3200
AC_BK	15	1023	7	0
AC_VI	7	15	2	6016
AC_VO	3	7	2	3264

---End

Parameter description

Parameter	Description
WMM	<ul style="list-style-type: none"> - Enable: It is used to enable the WMM function. - Disable: It is used to disable the WMM function.
WMM Optimization Mode	<p>It specifies the WMM optimization modes supported by the AP:</p> <ul style="list-style-type: none"> - Optimized For Throughput: If 10 or less devices are connected to the AP, you are recommended to select this mode to increase device throughput. - Optimized For Capacity: If more than 10 devices are connected to the AP, you are recommended to select this mode to ensure device connectivity. - Custom: This mode enables you to set the WMM EDCA parameters for manual optimization.
No ACK	<p>This item appears only after you set your WMM Optimization Mode as Custom.</p> <ul style="list-style-type: none"> - If the box is ticked, the No ACK policy is adopted. - If the box is unticked, the Normal ACK policy is adopted.
EDCA Parameters	For details, refer to section 8.5.1 Overview .

8.6 Access Control

8.6.1 Overview

It specifies that you can allow/disallow wireless devices with specified MAC addresses to access the AP's WiFi networks. The AP supports the following MAC address filter modes:

- **Disable:** It indicates that the access control function is disabled. In this case, all wireless devices can access the AP's WiFi networks.
- **Allow:** It indicates that only the wireless devices with the specified MAC addresses can access the specific WiFi network of AP.
- **Disallow:** It indicates that only the wireless devices with the specified MAC addresses cannot access the specific WiFi network of AP.

8.6.2 Configuring access control

1. Choose **Wireless > Access Control**.
2. From the **SSID** drop-down list box, select the SSID on which the MAC address access control is implemented.
3. Select an access control mode from the **MAC Filter Mode** drop-down list box.
 - If you select **Disable**, the Access Control function will be disabled.
 - If you select **Allow** or **Disallow**, enter the MAC addresses you want to control in the access control list and click Add.
 - If you want to control a wireless device that has been connected to the AP, directly click **Add** corresponding to the device to add it to the access control list.
4. Click **Save**.

Access Control Administrator:admin

You can specify MAC address filter rules to allow or disallow wireless devices to connect to the wireless networks of the AP.

SSID: IP-COM_888888

MAC Filter Mode: Allow

Buttons: Save, Restore, Help

ID	MAC Address	IP	Connection Uptime	Add to List
1	C4:0B:CB:81:5D:11	192.168.0.189	00:00:14	Add

MAC Address: 4C : CC : 6A : AD : 14 : 53

Operation: Add

Access control list

Parameter description

Parameter	Description
SSID	It specifies the SSID on which the MAC address access control is implemented.

Parameter	Description
MAC Filter Mode	<p>It specifies the mode to disallow/allow device with specific MAC addresses to access the selected SSID, or allow all devices to access the selected SSID.</p> <ul style="list-style-type: none">– Disable: It indicates that access control function is disabled so that all devices can access the AP's WiFi networks.– Allow: It indicates that only the wireless devices in the access control list can access the specific WiFi network with the selected SSID.– Disallow: It indicates that only the wireless devices in the access control list cannot access the specific WiFi network with the selected SSID.

8.6.3 Example

Networking requirement

A WiFi network with a SSID **home** has been set up in a large apartment. However, it is required that only family members are allowed to connect to this WiFi network.

It is recommended for the administrator to configure AP's access control function. Assume that these family members have three wireless devices with the following three MAC addresses:

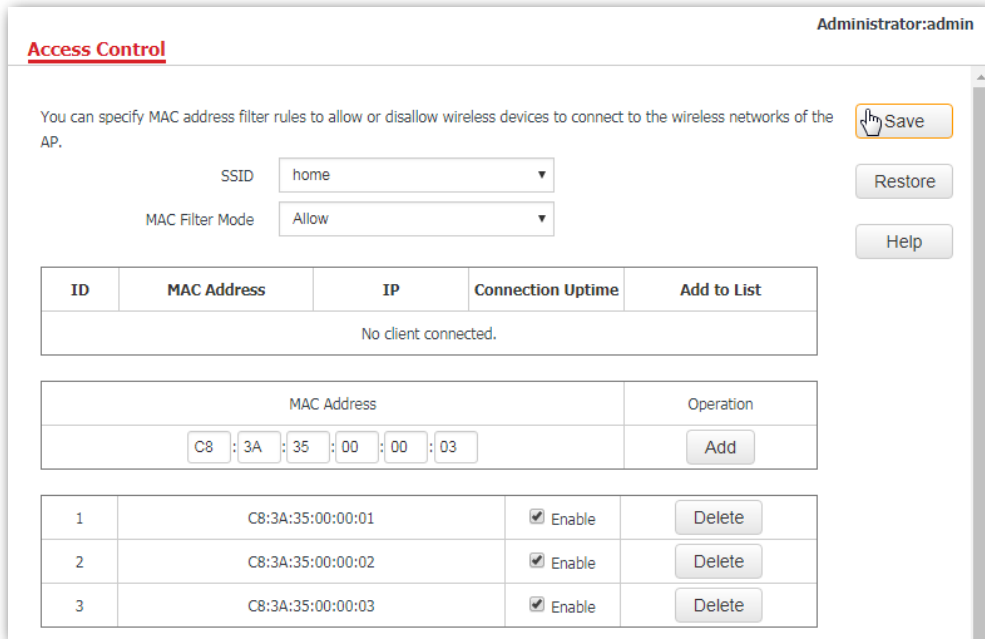
C8:3A:35:00:00:01

C8:3A:35:00:00:02

C8:3A:35:00:00:03.

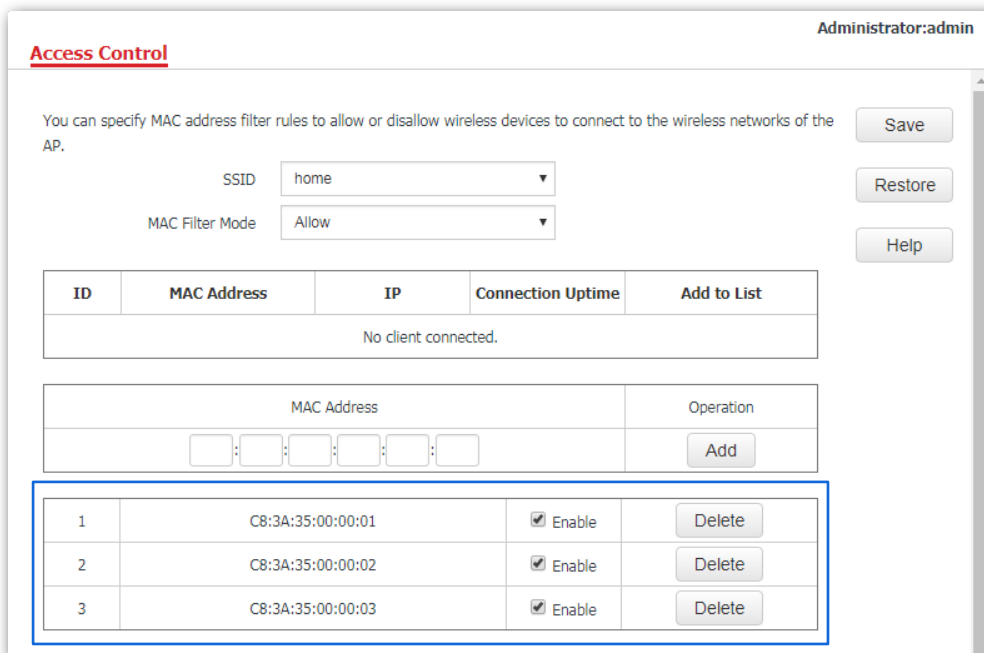
Procedures:

1. Choose **Wireless > Access Control**.
2. **SSID:** Select **home** from the **SSID** drop-down list box.
3. **MAC Filter Mode:** Select **Allow** from the drop-down list box.
4. **MAC Address:** Enter **C8:3A:35:00:00:01** in the **access control list** and click **Add**. Repeat this step to add **C8:3A:35:00:00:02** and **C8:3A:35:00:00:03** as well.
5. Click **Save**.



---End

The following figure shows the result after the configuration:



Verification

Only the three wireless devices on the access control list can connect to the **home** WiFi network.

8.7 Advanced

8.7.1 Overview

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

8.7.2 Changing the advanced settings



It is recommended that you'd better configure filtering WiFi networks' broadcast data only under the instructions of professional personnel, so as to prevent decreasing the WiFi performance of the AP.

In **Advanced** page, recognizing terminal type is not bound with filtering broadcast data function. It indicates that users are allowed to enable either recognizing terminal type or filtering broadcast data function, or enable both of them at the same time.

1. Choose **Wireless > Advanced**.
2. **Recognize Terminal Type**: Click **Enable**.
3. **Filter Broadcast Data**: Click **Enable**.
4. **Mode Option**: Select **Only accept DHCP and ARP packets** or **Only accept ARP packets** according to your requirement, which is **Only accept DHCP and ARP packets** in this example.
5. Click **Save**.

Administrator: admin

Advanced

Recognize Terminal Type Disable Enable

Filter Broadcast Data Disable Enable

Mode Option Only accept DHCP and ARP packets ▼

Save Restore Help

---End

Parameter description

Parameter	Description
Recognize Terminal Type	It specifies whether to recognize and display types of the devices connected to AP's WiFi networks. <ul style="list-style-type: none">– Disable: Click the circle beside it to disable the recognizing terminal type function.– Enable: Click the circle beside it to enable the recognizing terminal type function.
Filter Broadcast	It specifies whether to enable the filtering broadcast data function. By default, AP

Parameter	Description
Data	<p>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.</p> <ul style="list-style-type: none">- Disable: Click the circle beside it to disable the filtering broadcast data function.- Enable: Click the circle beside it to enable the filtering broadcast data function.
Mode Option	<p>It specifies what packets AP will accept after users enable filtering broadcast data function, consisting the following two modes:</p> <ul style="list-style-type: none">- Only accept DHCP and ARP packets: The AP will only accept data from DHCP and ARP packets.- Only accept ARP packets: The AP will only accept data from ARP packets.

8.8 QVLAN Setup

8.8.1 Overview

This AP supports the IEEE 802.1Q VLAN function and is able to 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.

8.8.2 Configuring the QVLAN function

1. Choose **Wireless > QVLAN Setup**.
2. Set the parameters as required. Generally, you only need to set the **Enable** and **VLAN ID** settings.
3. Click **Save**.

The screenshot shows the 'QVLAN Setup' configuration interface. At the top right, it says 'Administrator:admin'. The main area has a title 'QVLAN Setup' in red. Below the title, there are several settings: 'Enable' with a checked checkbox, 'PVID' with a text box containing '1', and 'Management VLAN' with a text box containing '1'. To the right of these settings are three buttons: 'Save', 'Restore', and 'Help'. Below these settings is a table with two columns: '2.4G SSID' and 'VLAN ID (1~4094)'. The table has one row with 'home' in the first column and '1000' in the second column.

---End

Parameter description

Parameter	Description
Enable	It specifies whether to enable the QVLAN function of the AP. By default, it is disabled.
PVID	It specifies the ID of the default native VLAN of the trunk port of the AP. The default value is 1 .
Management VLAN	It specifies the ID of the AP management VLAN. The default value is 1 . After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
2.4G SSID	It specifies the currently enabled SSID(s) of the AP.
VLAN ID	It specifies the VLAN IDs corresponding to SSIDs. The value range is 1 to 4094, and the default value is 1000 . 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>

8.8.3 Example

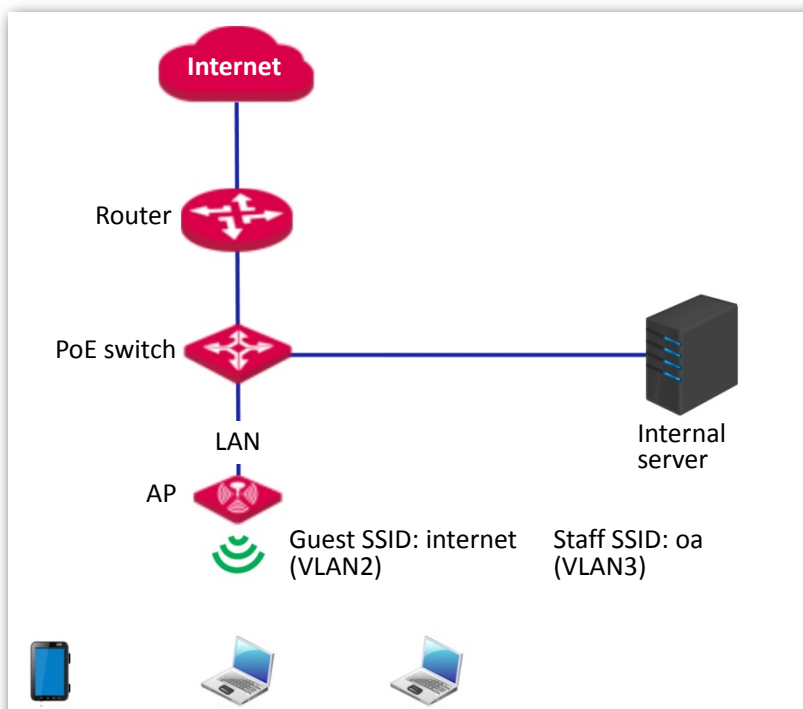
Networking requirement

A hotel has the following WiFi network coverage requirements:

- Guests are allowed to connect to VLAN 2 and only able to access the internet.
- Employees are allowed to connect to VLAN 3 and only able to access the LAN.

Assume that the SSID of the WiFi network for guests is **internet** and the SSID of the WiFi network for employees is **oa**.

Network topology



Procedures:

1. Configure the AP.
 - (1) Log in to the web UI of the AP and choose **Wireless > QVLAN Setup**.
 - (2) Select the **Enable** check box.
 - (3) Change the VLAN ID of the SSID **internet** to **2** and the VLAN ID of the SSID **oa** to **3**.
 - (4) Click **Save**.

The screenshot shows the 'QVLAN Setup' web interface. At the top right, it says 'Administrator:admin'. The main content area has a title 'QVLAN Setup' in red. Below the title, there are several configuration options: 'Enable' with a checked checkbox, 'PVID' with a text box containing '1', and 'Management VLAN' with a text box containing '1'. To the right of these options are three buttons: 'Save' (highlighted with a mouse cursor), 'Restore', and 'Help'. Below these options is a table with two columns: '2.4G SSID' and 'VLAN ID (1~4094)'. The table has two rows: one for 'internet' with a VLAN ID of '2', and one for 'oa' with a VLAN ID of '3'.

---End

Wait for the automatic reboot of the AP.

2. Configure the switch.

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

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

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

---End

Verification

Wireless devices connected to the SSID **internet** can access only the internet, whereas the wireless devices connected to the SSID **oa** can access only the LAN.

9 SNMP

9.1 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.

9.1.1 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.

9.1.2 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.

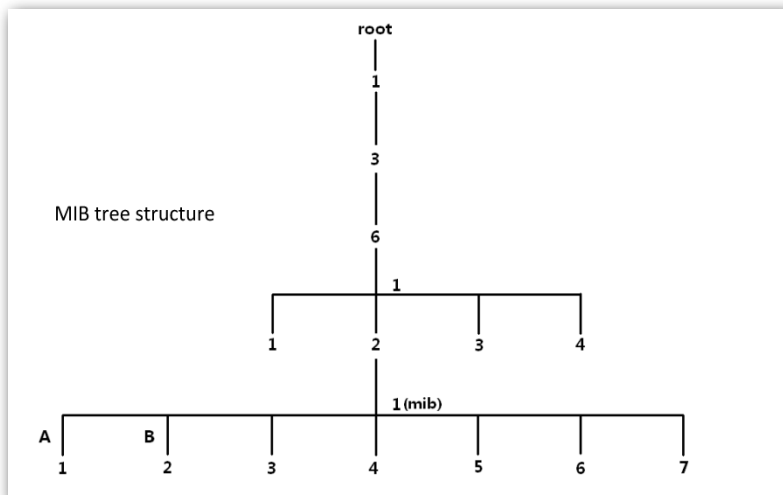
9.1.3 SNMP protocol version

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.

9.1.4 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.



9.2 Configuring the SNMP function

1. Click **SNMP** and set **SNMP Agent** to **Enable**.
2. Set related SNMP parameters.
3. Click **Save**.

SNMP Administrator:admin

You can configure SNMP V1 or SNMP V2C settings here.

SNMP Agent Disable Enable

Administrator

Device Name

Location


Read Community

Read/Write Community

Save Restore Help

---End

Parameter description

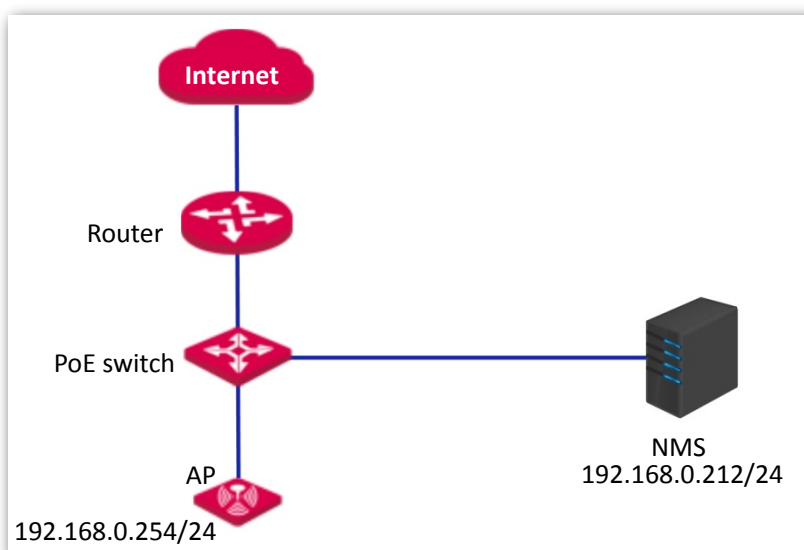
Parameter	Description
SNMP Agent	It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled. An SNMP manager and the SNMP agent can communicate with each other only when their SNMP versions are the same. Currently, the SNMP agent function of the AP supports SNMP V1 and SNMP V2C.
Administrator	It specifies the administrator's name of the AP. The default name is Administrator . You can change the administrator's name if required.
Device Name	It specifies the device name of the AP. By default, the device name is Wireless Access Point . You can change it if required.  Tip You are recommended to change the AP name so that you can identify your AP easily when managing the AP using SNMP.
Location	It specifies the location where the AP is used. You can change 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 public . 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 private . The SNMP agent function of the AP allows an SNMP manager to use the password

Parameter	Description
	to read/write variables in the MIB of the AP.

9.3 Example

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.

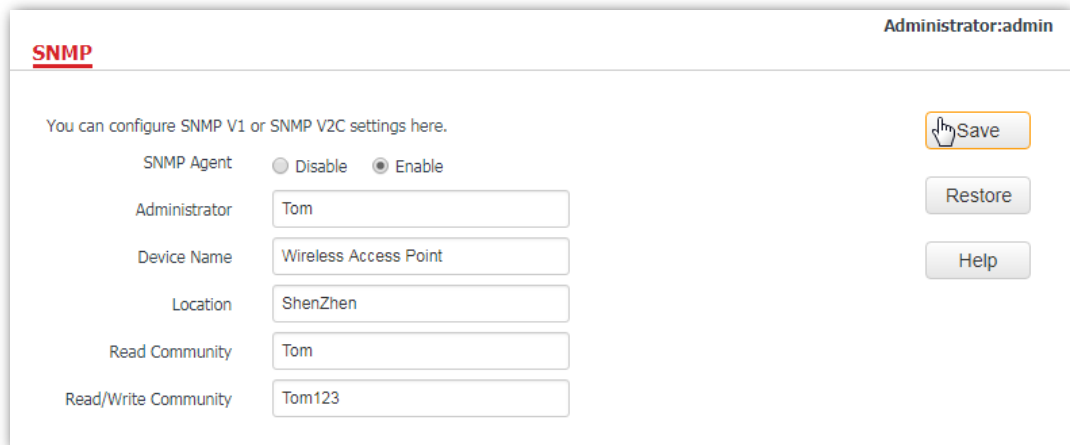


Procedure:

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**.



The screenshot shows the SNMP configuration page in a web interface. The page title is "SNMP" and the user is logged in as "Administrator:admin". The main heading says "You can configure SNMP V1 or SNMP V2C settings here." Below this, there are several configuration fields and a "SNMP Agent" section. The "SNMP Agent" section has two radio buttons: "Disable" and "Enable", with "Enable" selected. The "Administrator" field contains "Tom". The "Device Name" field contains "Wireless Access Point". The "Location" field contains "ShenZhen". The "Read Community" field contains "Tom". The "Read/Write Community" field contains "Tom123". On the right side of the form, there are three buttons: "Save" (highlighted with a mouse cursor), "Restore", and "Help".

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.

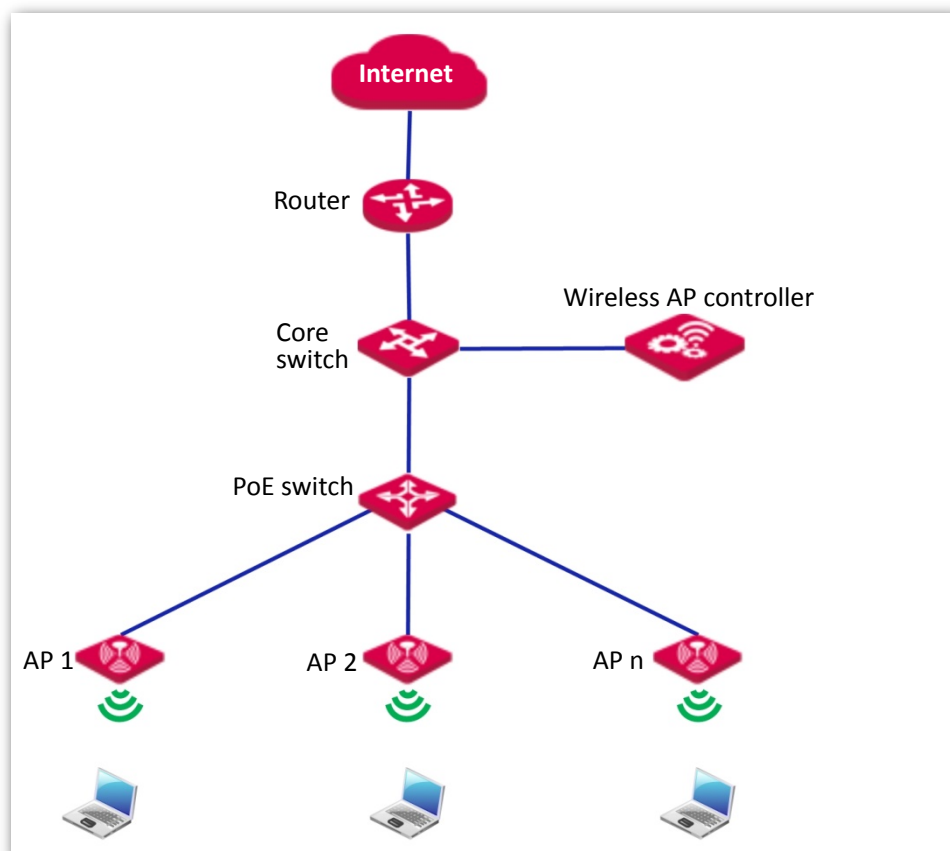
10 Deployment

10.1 Overview

If a large number of APs are deployed, you are recommended to adopt an IP-COM AP controller to manage the APs in a centralized manner, such as AC1000/2000/3000. The AP supports two deployment modes: local deployment and cloud deployment. By default, the AP is in local deployment mode.

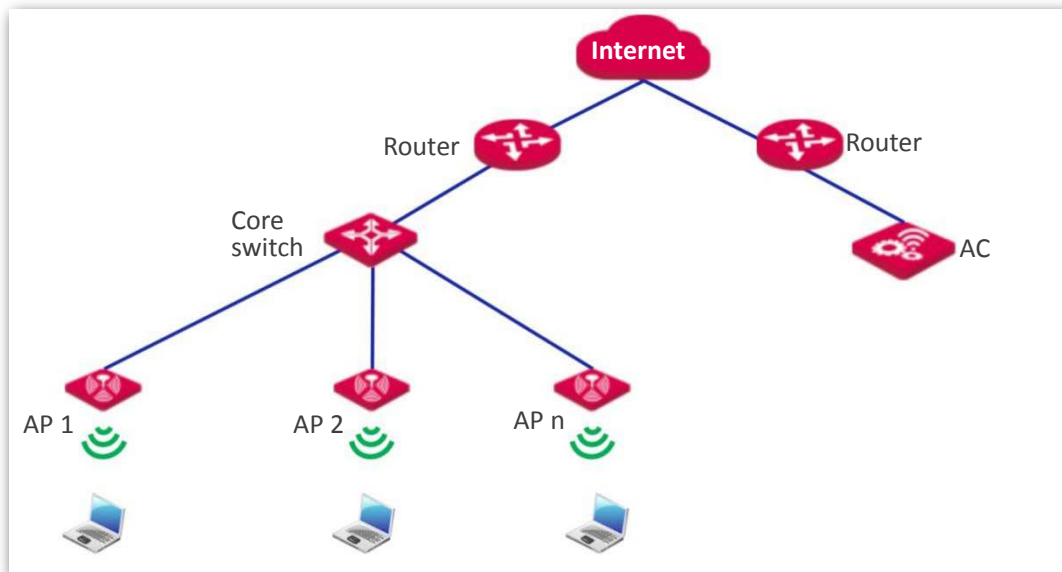
- **Local deployment**

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.



10.2 Configuring the deployment mode

10.2.1 Configuring the local deployment mode

1. Click **Deployment**, and select **Local**.
2. Click **Save**.

The screenshot shows the 'Deployment' configuration page with the 'Local' radio button selected. The 'Device Name' field contains 'Wireless Access Point'. The 'Cloud AC Address' field is empty, with a note: '(The WAN IP address of the router that the Root AC connects to)'. The 'Cloud AC Manage Port' and 'Cloud AC Upgrade Port' fields are empty, both with a note: '(Valid Range: 1024~65535)'. On the right side, there are three buttons: 'Save' (highlighted with a yellow border), 'Restore', and 'Help'. The top right corner shows 'Administrator:admin'.

---End

10.2.2 Configuring the cloud deployment mode

1. Click **Deployment**, and select **Cloud**.
2. Set related parameters, including device name, cloud AC address, cloud AC manage port and cloud AC upgrade port.
3. Click **Save**.

The screenshot shows the 'Deployment' configuration page with the 'Cloud' radio button selected. The 'Device Name' field contains 'Wireless Access Point'. The 'Cloud AC Address' field is empty, with a note: '(The WAN IP address of the router that the Root AC connects to)'. The 'Cloud AC Manage Port' and 'Cloud AC Upgrade Port' fields are empty, both with a note: '(Valid Range: 1024~65535)'. On the right side, there are three buttons: 'Save', 'Restore', and 'Help'. The top right corner shows 'Administrator:admin'.

---End

Parameter description

Parameter	Description
Deployment	It specifies the deployment mode of the AP. The default option is Local . <ul style="list-style-type: none">– Local: It indicates that the AP can be managed only through the AC connected to the same local network.

Parameter	Description
	<ul style="list-style-type: none">– Cloud: In this mode, the AP can be managed only by a cloud AC or a cloud server. To adopt the cloud deployment mode, you should set the device name, cloud AC address, cloud AC manage port and cloud AC upgrade port for your AP as well.
Device Name	It specifies the device name of the AP. You are recommended to change the device name so that you can quickly locate the AP when managing the AP remotely.
Cloud AC Address	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.
Cloud AC Manage Port	It specifies the port of the router to which the cloud AC connects for managing APs.
Cloud AC Upgrade Port	It specifies the port of the router to which the cloud AC connects for upgrading APs.

11 Tools

11.1 Firmware Upgrade

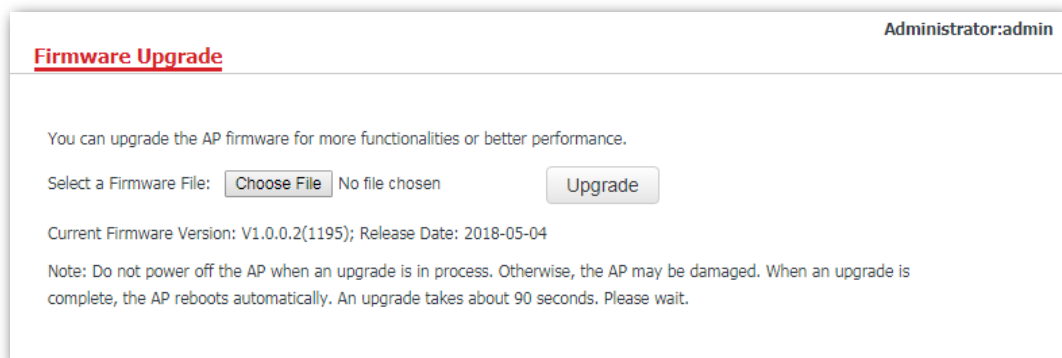
This function enables users to upgrade the AP's firmware for more functions and higher stability.



To prevent damaging the AP, ensure that the new firmware version is applicable to the AP before upgrading the firmware, and keep powering on the AP during an upgrade.

Procedures:

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 and click **Tools > Firmware Upgrade**.
3. Click **Choose File** and select the downloaded firmware file for upgrade.
4. Click **Upgrade**.



The screenshot shows a web interface titled "Firmware Upgrade" with the administrator name "Administrator:admin" in the top right corner. The main content area contains the following text: "You can upgrade the AP firmware for more functionalities or better performance." Below this is a "Select a Firmware File:" label followed by a "Choose File" button, the text "No file chosen", and an "Upgrade" button. Underneath, it displays "Current Firmware Version: V1.0.0.2(1195); Release Date: 2018-05-04". A note at the bottom states: "Note: Do not power off the AP when an upgrade is in process. Otherwise, the AP may be damaged. When an upgrade is complete, the AP reboots automatically. An upgrade takes about 90 seconds. Please wait."

---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.



After the firmware is upgraded, you are recommended to restore the factory settings of the AP and configure the AP again, so as to ensure stability of the AP and proper operation of new functions.

11.2 Date & Time

This module enables you to set the system time and login timeout interval of your AP.

11.2.1 System Time

Ensure that the system time of the AP is correct, so that logs can be recorded correctly and the reboot schedule can be executed correctly.

To access the page, click **Tools > Date & Time**.

Administrator:admin

System Time Login Timeout

You can configure the system time of the AP here.

Note: The system time is lost when the AP is turned off. It will be synchronized with the GMT time automatically when the AP is turned on and connected to the internet again.

Synchronize with internet time Sync Interval: 30 minutes

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei

Note: The system is automatically synchronized with the GMT time only after the AP is connected to the Internet.

Enter Date and Time:

2018 Y 05 M 23 D 15 h 24 m 26 s Synchronize with PC Time

Save

Restore

Help

The AP allows you to set its system time by synchronizing the time with the internet or setting the time manually. By default, the AP is configured to synchronize the system time with the internet.

Parameter description

Parameter	Description
Synchronize with internet time	Tick the box beside this item to synchronize the AP's system time with the internet time.
Sync Interval	It specifies the interval at which the AP synchronizes its system time with the internet time.
Synchronize with PC Time	Click this parameter to synchronize the AP's system time with the system time of the computer used to manage the AP.

Configuring AP to synchronizing with internet time

The AP automatically synchronizes its system time with a time server of the internet, which enables the AP to correct its system time automatically after being connected to the internet.

For details about how to connect the AP to the internet, refer to [Quick setup](#).

Procedures:

1. Click **Tools > Date & Time > System Time**.
2. Tick the **Synchronize with internet time** box.
3. **Sync Interval**: Select a desired value from the drop-down-list box. The default value **30 minutes** is recommended.
4. Set **Time Zone** to the time zone of your location.
5. Click **Save**.

The screenshot shows the 'System Time' configuration page. At the top right, it says 'Administrator:admin'. The page has two tabs: 'System Time' (selected) and 'Login Timeout'. Below the tabs, there is a text box: 'You can configure the system time of the AP here.' To the right of this text is a 'Save' button. Below that is a note: 'Note: The system time is lost when the AP is turned off. It will be synchronized with the GMT time automatically when the AP is turned on and connected to the internet again.' The main configuration area is enclosed in a blue border and contains: a checked checkbox for 'Synchronize with internet time', a 'Sync Interval' dropdown menu set to '30 minutes', and a 'Time Zone' dropdown menu set to '(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei'. Below this is another note: 'Note: The system is automatically synchronized with the GMT time only after the AP is connected to the Internet.' To the right of the configuration area are 'Restore' and 'Help' buttons. At the bottom, there is a section 'Enter Date and Time:' with input fields for Year (2018), Month (05), Day (23), Hour (15), Minute (43), and Second (46), and a 'Synchronize with PC Time' button.

---End

Configuring date and time manually for AP

Users can manually set the system time for APs. If you choose to set date and time for your AP manually, you need to set the system time each time after the AP reboots.

Procedures:

1. Click **Tools > Date & Time > System Time**.
2. Enter a correct date and time, or click **Synchronize with PC Time** to synchronize the system time of the AP with the system time of the computer used to manage the AP.
3. Click **Save**.

System Time Login Timeout Administrator:admin

You can configure the system time of the AP here.

Note: The system time is lost when the AP is turned off. It will be synchronized with the GMT time automatically when the AP is turned on and connected to the internet again.

Synchronize with internet time Sync Interval: 30 minutes

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei

Note: The system is automatically synchronized with the GMT time only after the AP is connected to the Internet.

Enter Date and Time:

2018 Y 05 M 23 D 15 h 58 m 26 s Synchronize with PC Time

Save Restore Help



Note

If you decide to synchronize the system time of the AP with the system time of the computer used to manage the AP, make sure the computer's system time is correct.

---End

11.2.2 Login Timeout

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. The default login timeout interval is 5 minutes.

Configuring the login timeout interval:

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

System Time **Login Timeout** Administrator:admin

Login Timeout: 10 minute (Range: 1 - 60)

Save Restore Help

---End

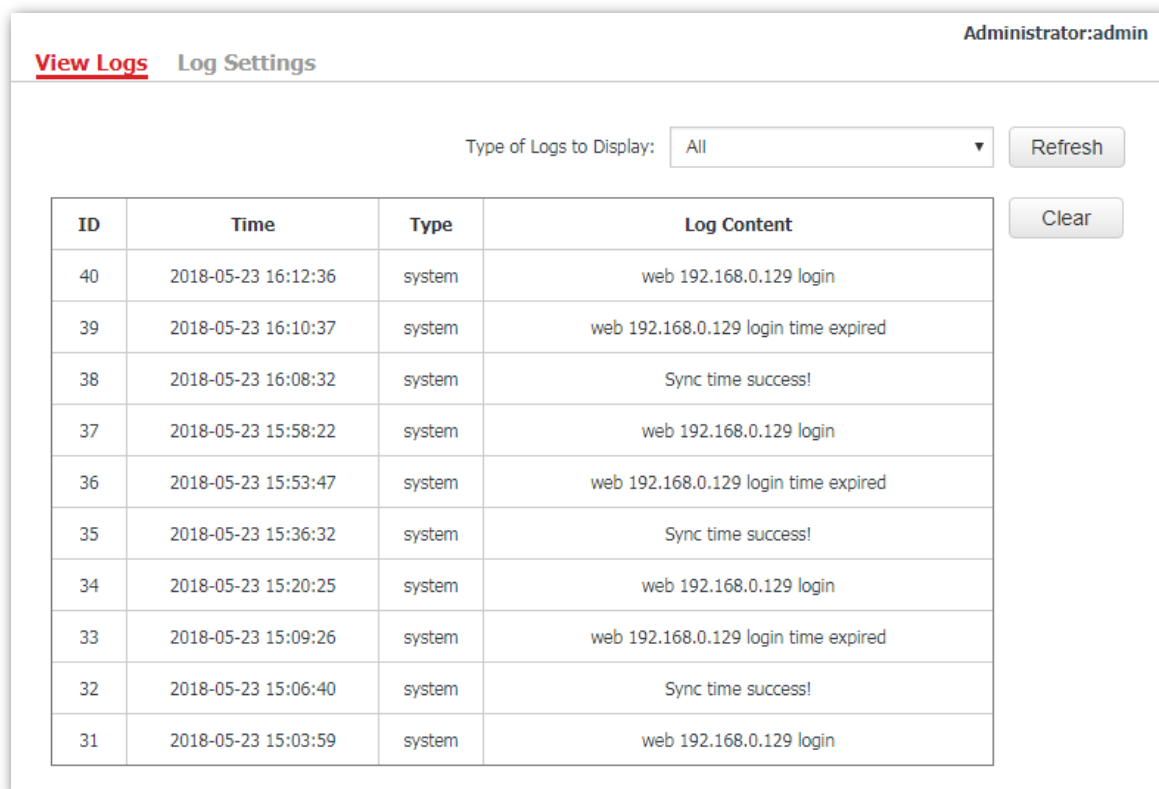
11.3 Logs

This module enables you to view logs and configure log settings.

11.3.1 View Logs

Logs record various events that occur to the AP and the operations that users perform on the AP after the AP starts. In case of system faults, refer to the logs during troubleshooting.

To access the page, click **Tools > Logs > View Logs**.



The screenshot shows the 'View Logs' interface. At the top right, it says 'Administrator:admin'. Below that, there are two tabs: 'View Logs' (which is active) and 'Log Settings'. Under the 'View Logs' tab, there is a dropdown menu labeled 'Type of Logs to Display:' with 'All' selected. To the right of the dropdown are two buttons: 'Refresh' and 'Clear'. Below this is a table with four columns: 'ID', 'Time', 'Type', and 'Log Content'. The table contains 10 rows of log entries, with IDs ranging from 40 down to 31. The log content includes messages like 'web 192.168.0.129 login', 'web 192.168.0.129 login time expired', and 'Sync time success!'.

ID	Time	Type	Log Content
40	2018-05-23 16:12:36	system	web 192.168.0.129 login
39	2018-05-23 16:10:37	system	web 192.168.0.129 login time expired
38	2018-05-23 16:08:32	system	Sync time success!
37	2018-05-23 15:58:22	system	web 192.168.0.129 login
36	2018-05-23 15:53:47	system	web 192.168.0.129 login time expired
35	2018-05-23 15:36:32	system	Sync time success!
34	2018-05-23 15:20:25	system	web 192.168.0.129 login
33	2018-05-23 15:09:26	system	web 192.168.0.129 login time expired
32	2018-05-23 15:06:40	system	Sync time success!
31	2018-05-23 15:03:59	system	web 192.168.0.129 login

To ensure that the logs are recorded correctly, make sure that AP's system time is correct. You can correct the system time by clicking **Tools > Time & Date > System Time**.

To view the latest logs of the AP, click **Refresh**. To clear the current logs, click **Clear**.

Note

When the AP reboots, the previous logs are lost. And the AP reboots when one of the followings happens: the AP is powered on after a power failure; the QVLAN function is configured; the firmware is upgraded; an AP configuration is backed up or restored or the AP is restored to factory settings.

11.3.2 Configuring log settings

To access the page, click **Tools > Logs > Log Settings**.

On this page, you can set the number of displayed logs and configure the log server function.

Administrator:admin

View Logs Log Settings

Number of Logs Displayed (Range: 100 - 300; Default: 150)

Enable Log Server Function

ID	Log Server IP Address	Log Server Port	Enable	Operation
----	-----------------------	-----------------	--------	-----------

Setting the number of displayed logs

By default, the AP can display a maximum of 150 logs on the **View Logs** page. You can change the number as required.

Procedure:

1. To access the page, click **Tools > Logs > Log Settings**.
2. **Number of Logs Displayed:** Change the number of logs as required within the range of 100 to 300.
3. Click **Save**.

Administrator:admin

View Logs Log Settings

Number of Logs Displayed (Range: 100 - 300; Default: 150)

Enable Log Server Function

ID	Log Server IP Address	Log Server Port	Enable	Operation
----	-----------------------	-----------------	--------	-----------

---End

Configuring the log server settings

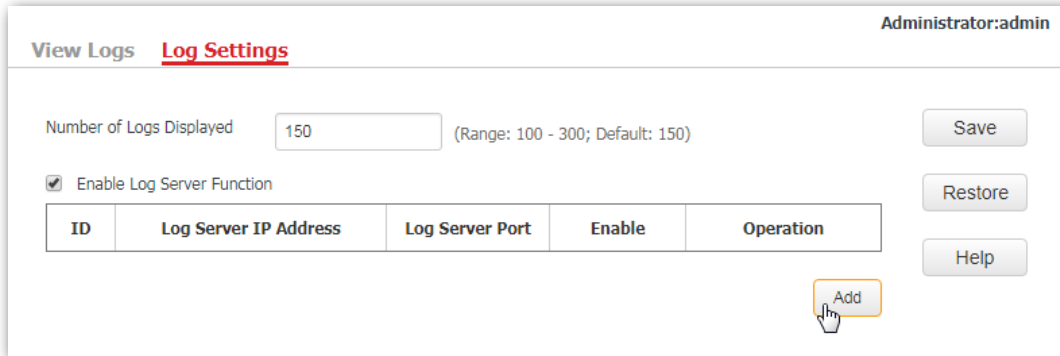
After you specify a log server, the AP sends its logs to the log server. You can view all the historical logs of the AP on the log server.



To ensure that system logs can be sent to a log server, choose **Network > LAN Setup** and set the IP address, subnet mask, and gateway of the AP to communicate with the log server.

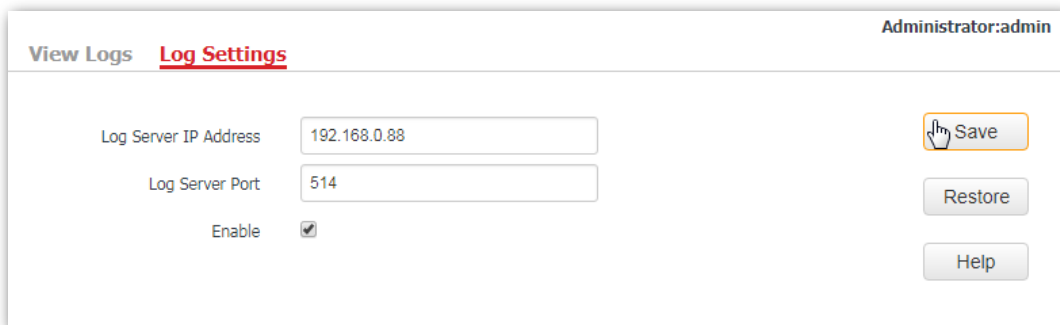
Adding a log server

1. To access the page, click **Tools > Logs > Log Settings**.
2. Tick the box beside the **Enable Log Server Function** item.
3. Click **Add**.



The screenshot shows the 'Log Settings' page with the 'Enable Log Server Function' checkbox checked. The 'Number of Logs Displayed' is set to 150. A table with columns 'ID', 'Log Server IP Address', 'Log Server Port', 'Enable', and 'Operation' is visible. The 'Add' button is highlighted with a mouse cursor.

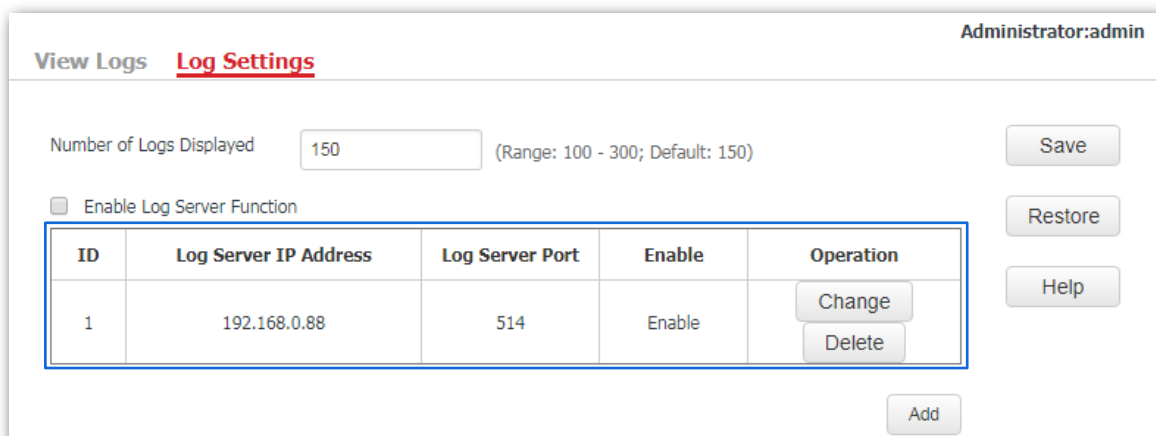
4. Set parameters as follows:
 - **Log Server IP Address:** Enter the IP address of your log server, which is **192.168.0.88** in this example.
 - **Log Server Port:** Enter the log server's UDP port number used to send and receive system logs. The default port number 514 is recommended.
 - **Enable:** Tick the box to enable the log server.
5. Click **Save**.



The screenshot shows the 'Log Settings' page with the 'Log Server IP Address' field set to 192.168.0.88, the 'Log Server Port' field set to 514, and the 'Enable' checkbox checked. The 'Save' button is highlighted with a mouse cursor.

---End

The following figure shows the configuration:



The screenshot shows the 'Log Settings' page with the 'Enable Log Server Function' checkbox unchecked. The 'Number of Logs Displayed' is set to 150. A table with columns 'ID', 'Log Server IP Address', 'Log Server Port', 'Enable', and 'Operation' is visible. The table contains one row with ID 1, IP Address 192.168.0.88, Port 514, and Enable checked. The 'Change' and 'Delete' buttons are visible in the 'Operation' column. The 'Add' button is highlighted with a mouse cursor.

ID	Log Server IP Address	Log Server Port	Enable	Operation
1	192.168.0.88	514	Enable	Change Delete

Changing log server settings

1. To access the page, click **Tools > Logs > Log Settings**.
2. Click **Change** corresponding to the log server settings to be changed.
3. Change the parameter settings as required.
4. Click **Save**.

---End

Deleting log server settings

1. To access the page, click **Tools > Logs > Log Settings**.
2. Click **Delete** corresponding to the log server settings to be deleted.

---End

11.4 Configuration

This module enables you to back up the current configuration of the AP, restore a previous configuration of the AP, and restore the AP to factory settings.

11.4.1 Backup and restoring configurations

The backup function enables you to back up the current configuration of the AP to a local computer. The restoration function enables you to restore the AP to previous configuration.

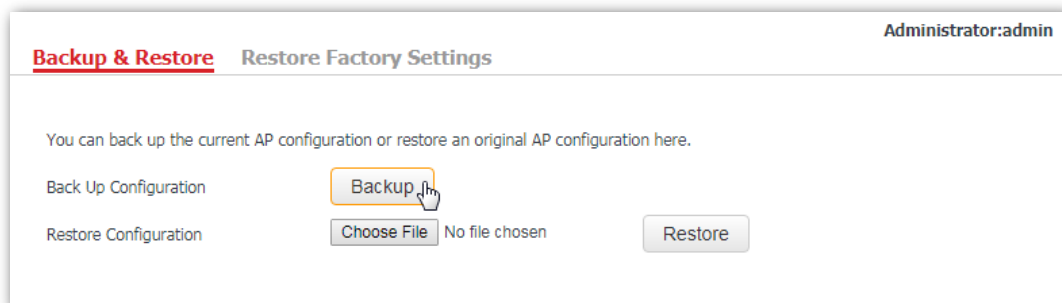
If the AP enters the optimum condition after you greatly change the configuration of the AP, you are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the AP.



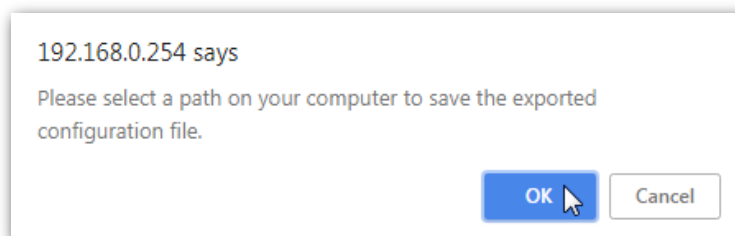
If you need to apply same or similar configuration to many APs, you can configure one of the APs, back up its configuration, and use the backup configuration file to restore the configuration of other APs.

Backup the current configuration

1. Click **Tools > Configuration > Backup & Restore**.
2. Click **Backup** and follow the on-screen instructions to perform operations.



3. Click **OK**.



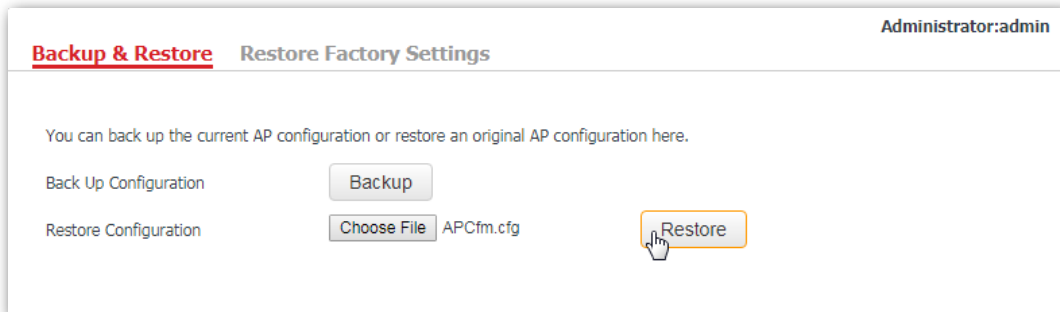
---End

Verification

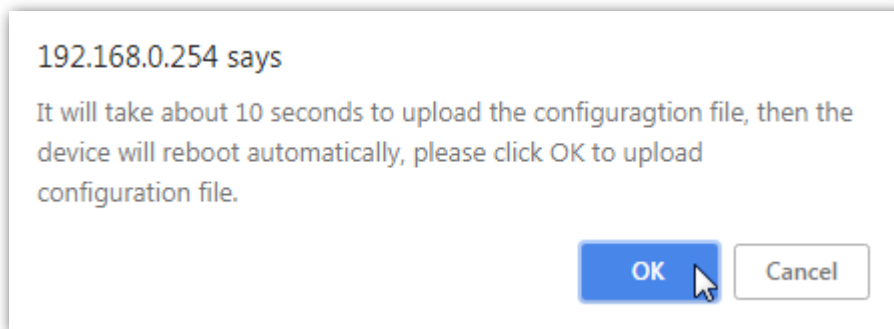
A configuration file called as **APCfm.cfg** will be downloaded.

Restoring previous configuration

1. Click **Tools > Configuration > Backup & Restore**.
2. Click **Choose File** and select the configuration file to be restored.
3. Click **Restore** and follow the on-screen instructions to perform operations.



4. Click **OK**.



---End

Verification

A progress bar will appear after you click **OK**. And the AP is restored to previous configuration after the progress bar ends.

11.4.2 Restoring the AP to factory settings

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

After you reset the AP, the login IP address of the AP is changed to **192.168.0.254**, and the user name and password of the AP are changed to **admin**.

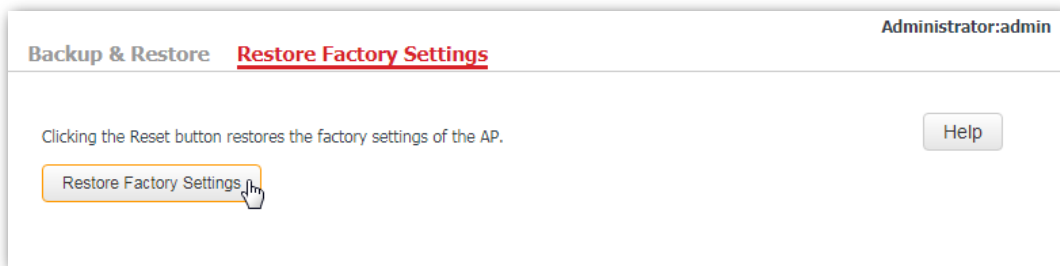


AP's configuration is lost if you restore it to the factory settings. And you need to reconfigure the AP to connect to the internet. Therefore, restore the factory settings of the AP only when necessary.

To prevent damages, ensure that the AP is connected to power supply properly when the AP is reset.

Restoring the factory settings using web UI

1. Click **Tools > Configuration** and click the **Restore Factory Settings** tab.
2. Click the **Restore Factory Settings** button.

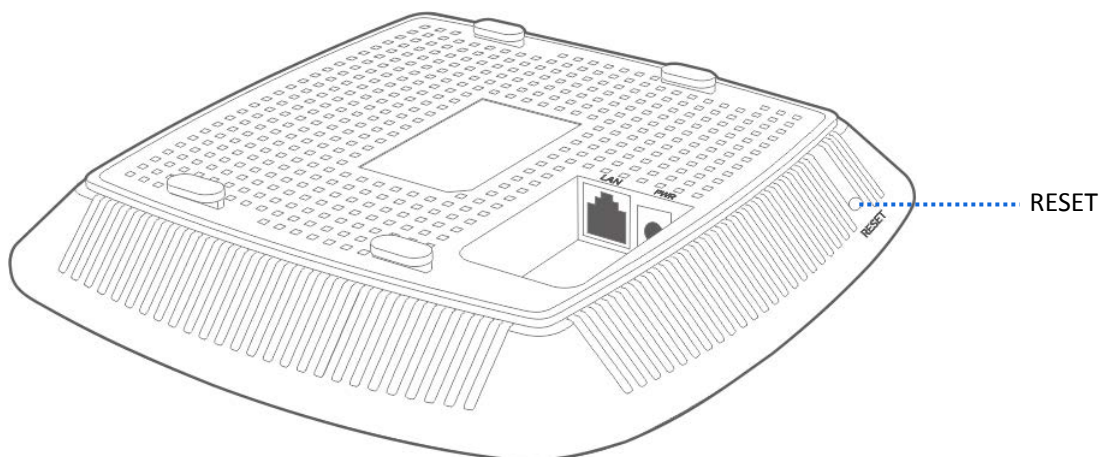


---End

Restoring the factory settings using hardware

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

After the LED indicator blinks, hold down the RESET button for about 8 seconds. The AP is reset successfully when the LED indicator gets solid on.



11.5 Account

This page enables you to change the AP's login account information such as user name and password to prevent unauthorized login.


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

Account Administrator:admin

You can change your login user name and password here.
Note: Only 1 to 32 letters, digits, and underscores are allowed in a user name or password.

Account Type	User Name	Enable	Operation
Administrator	admin	<input checked="" type="checkbox"/>	<input type="button" value="Change"/>
User	user	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/> <input type="button" value="Change"/>

Parameter description

Parameter	Description
Access Type	<p>It specifies the account used to log in to the AP's web UI.</p> <ul style="list-style-type: none">- Administrator: It specifies the account enabling you to view and modify settings of the AP.- User: It specifies the account only enabling you to view settings of the AP.
User Name	<p>It specifies the user name of an account.</p> <p>By default, the AP has one administrator account and one user account. Both the default user name and password of the administrator account are admin, and both the user name and password of the user account are user.</p>
Enable	<p>It specifies whether an account is enabled.</p> <ul style="list-style-type: none">- The administrator account is enabled for all time.- The user account is enabled by default but you can disable it if required.
Operation	<p>Change: Used to change the user name and password of the account corresponding to the button.</p> <p>Delete: Used to delete the user account.</p> <p> Note</p> <p>Changing, deleting, or adding an account succeeds only after you click Save.</p>

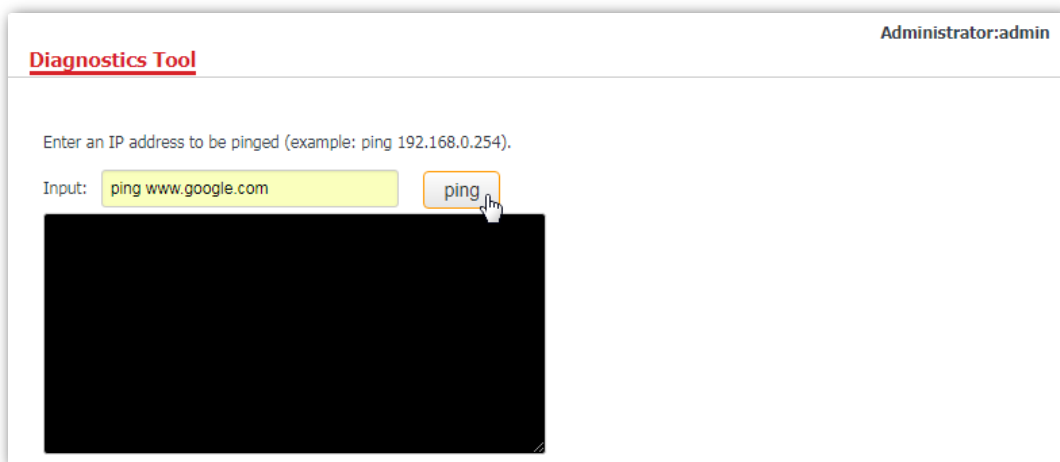
11.6 Diagnostics Tool

If the network connection fails, you can use the diagnostics tool included in the AP to locate the faulty node.

11.6.1 Locating the faulty node

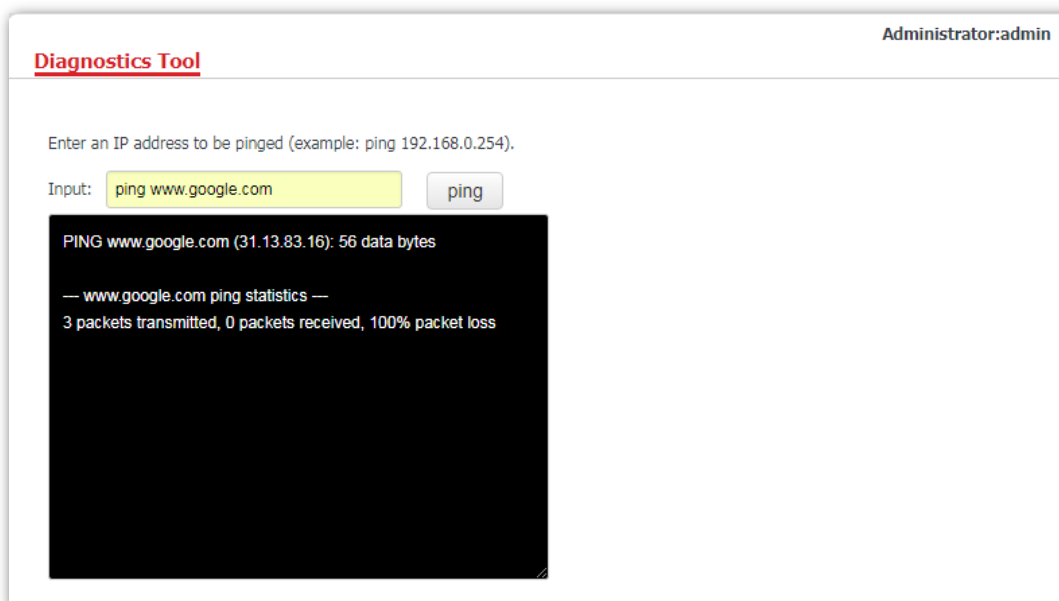
The link `www.google.com` is used as an example.

1. Click **Tools > Diagnostics Tool**.
2. Enter the IP address or domain name to be pinged in the **Input** box, which is `ping www.google.com` in this example.
3. Click **Ping**.



---End

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



11.7 Device Reboot

This module enables you to manually reboot the AP or configure the AP to reboot automatically.



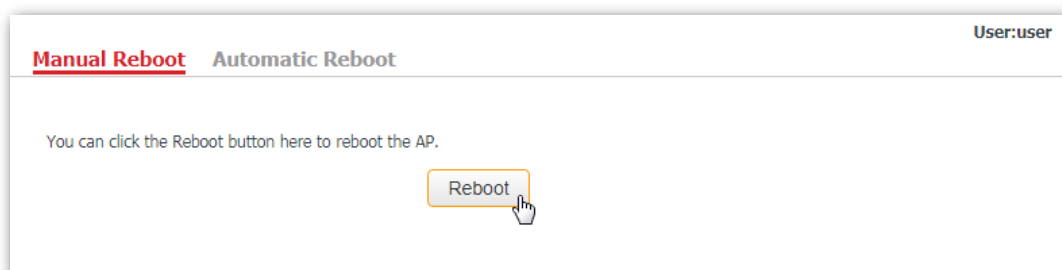
When the AP reboots, all connections are released. You are recommended to reboot the AP in spare time.

11.7.1 Manual reboot

If a setting does not take effect, you can try rebooting the AP to resolve the problem.

Procedures:

1. To access the page, click **Tools > Device Reboot**.
2. Click **Reboot**.



---End

11.7.2 Automatic reboot

This function enables the AP to reboot automatically as scheduled. You can use this function to prevent wireless performance degradation or network instability that occurs after AP is online for a long time. The AP can reboot:

- **At intervals:** In this mode, the AP reboots at the interval you set.
- **At specified time:** In this mode, the AP reboots regularly at the time you set.

Configuring the AP to reboot at an interval

1. Click **Tools > Device Reboot** and click the **Automatic Reboot** tab.
2. Tick the **Enable Auto Reboot** box.
3. **Reboot Mode:** Select **At Intervals**.
4. **Interval:** Set your required value, such as **1440** in this example.
5. Click **Save**.

The screenshot shows the 'Automatic Reboot' configuration page. At the top right, it says 'User:user'. Below the title, there are two tabs: 'Manual Reboot' and 'Automatic Reboot', with the latter being selected. The 'Enable Auto Reboot' checkbox is checked. The 'Reboot Mode' dropdown menu is set to 'At intervals'. The 'Interval' input field contains the value '1440', with a note 'minute (Range: 10 - 7200)'. On the right side, there are three buttons: 'Save' (highlighted with a mouse cursor), 'Restore', and 'Help'.

---End

Configuring the AP to reboot at specified time

1. Click **Tools > Device Reboot** and click the **Automatic Reboot** tab.
2. Tick the **Enable Auto Reboot** box.
3. **Reboot Mode:** Select **At specified time**
4. **Date:** Select the required day(s) when the AP reboots, which is **Mon.** in this example.
5. **Time:** Set the time when the AP reboots, which is **24:00** in this example.
6. Click **Save**.

The screenshot shows the 'Automatic Reboot' configuration page. At the top right, it says 'User:user'. Below the title, there are two tabs: 'Manual Reboot' and 'Automatic Reboot', with the latter being selected. The 'Enable Auto Reboot' checkbox is checked. The 'Reboot Mode' dropdown menu is set to 'At specified time'. The 'Date' section has radio buttons for 'Every day', 'Mon.', 'Tue.', 'Wed.', 'Thur.', 'Fri.', 'Sat.', and 'Sun.', with 'Mon.' selected. The 'Time' input field contains the value '24:00', with an example 'Example: 3:00'. On the right side, there are three buttons: 'Save' (highlighted with a mouse cursor), 'Restore', and 'Help'.

---End

11.8 LED Control

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

Turning off the LED indicator:

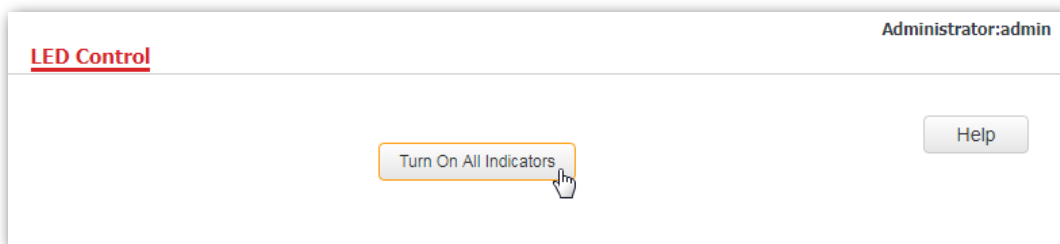
1. Click **Tools > LED Control**.
2. Click **Turn Off All Indicators**.



---End

Turning on the LED indicator:

1. Click **Tools > LED Control**.
2. Click **Turn On All Indicators**.



---End



Note

The button **Turn On All Indicators** only appears after the AP's LED indicator is turned off. By default, the LED indicator is turned on.

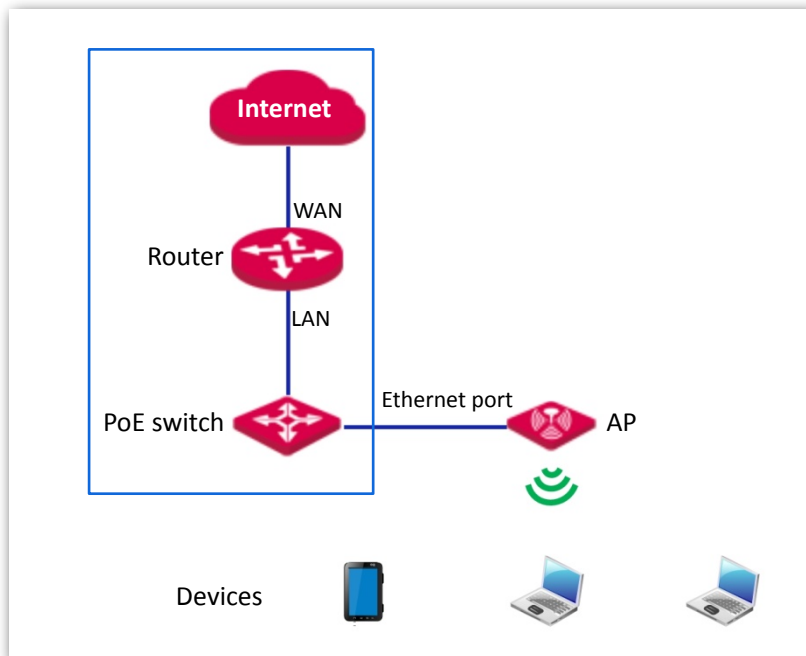
11.9 Uplink Detection

11.9.1 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 detection 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).



11.9.2 Configuring uplink detection

1. Click **Tools > Uplink Detection**.
2. **Uplink Detection**: Tick the **Enable** box.
3. **Host 1 to Be Pinged/Host 2 to Be Pinged**: Enter the IP address(es) of the host to be pinged through the LAN port of the AP, such as the IP address of the switch or router directly connected to the AP.
4. **Pinging Interval**: Enter the interval at which the AP detects its uplink.
5. Click **Save**.

Administrator:admin

Uplink Detection

Uplink Detection	<input checked="" type="checkbox"/> Enable	<input type="button" value="Save"/>
Host 1 to Be Pinged	<input type="text" value="192.168.0.1"/>	<input type="button" value="Restore"/>
Host 2 to Be Pinged	<input type="text"/>	<input type="button" value="Help"/>
Pinging Interval	<input type="text" value="10"/> minute (Range: 10 - 100)	

---End




Host 1 to Be Pinged is not bound with **Host 2 to Be Pinged**, which indicates that you can enter IP address either in **Host 1 to Be Pinged** or **Host 2 to Be Pinged**, or enter IP addresses for both of these two parameters.

Appendix A

Configuring a static IP address for your computer (Example: Win7)

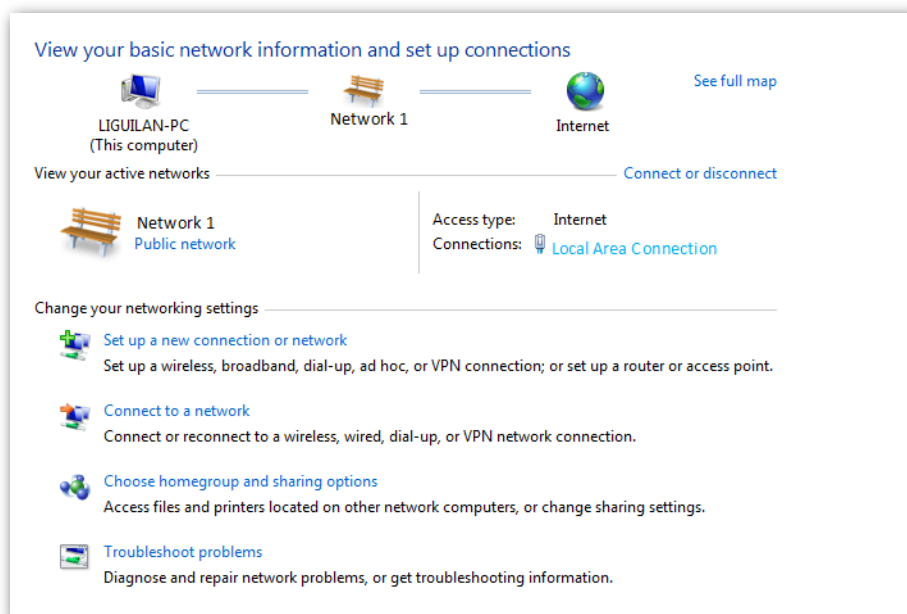
Procedures:

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

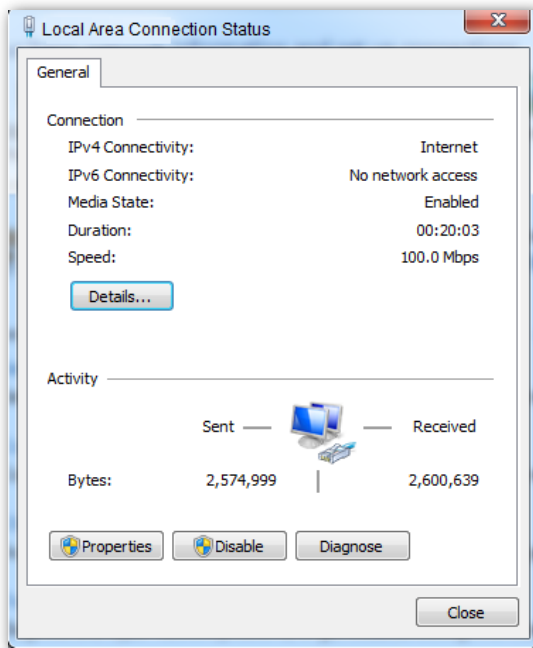


Open Network and Sharing Center

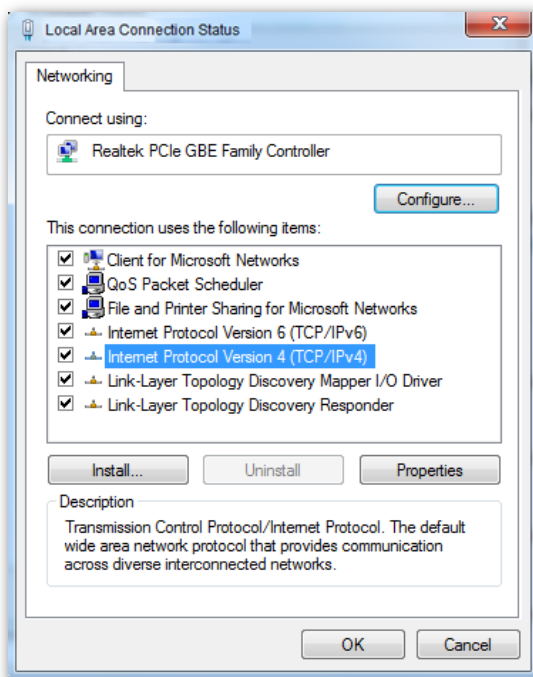
2. Click **Local Area Connection**.



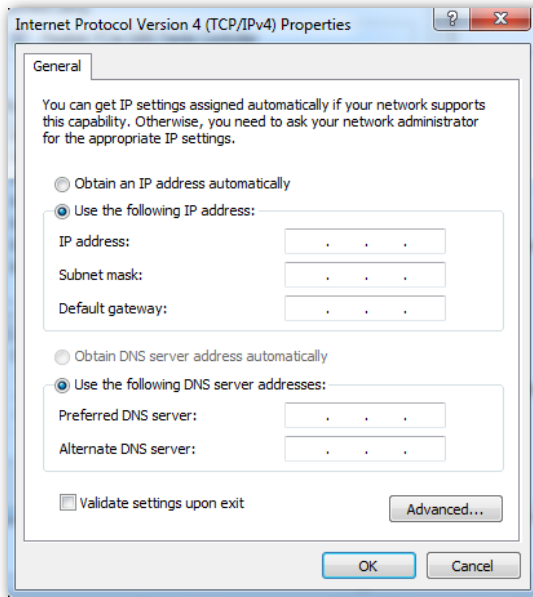
3. Click **Properties**.



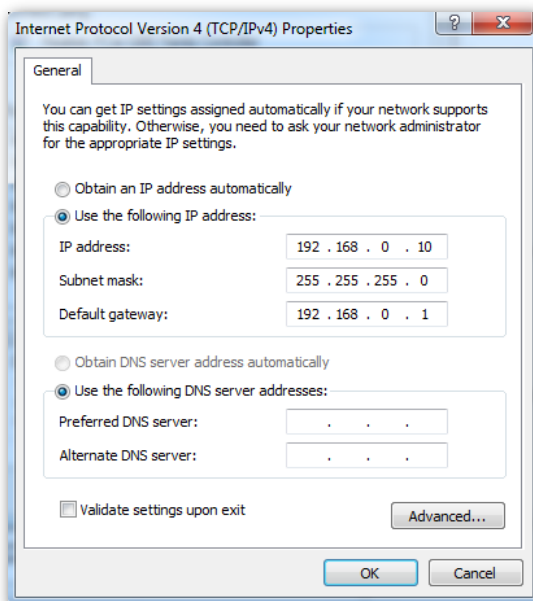
4. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



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



6. **IP address, Subnet mask, Default gateway:** Enter the static IP address, subnet mask and default gateway you set for your computer, which is **192.168.0.10**, **255.255.255.0** and **192.168.0.1** respectively in this example, and click **OK**.




 **Note**

Default gateway is the LAN IP address of the upstream device through which your computer can access the internet, such as the router to which your computer is connected.

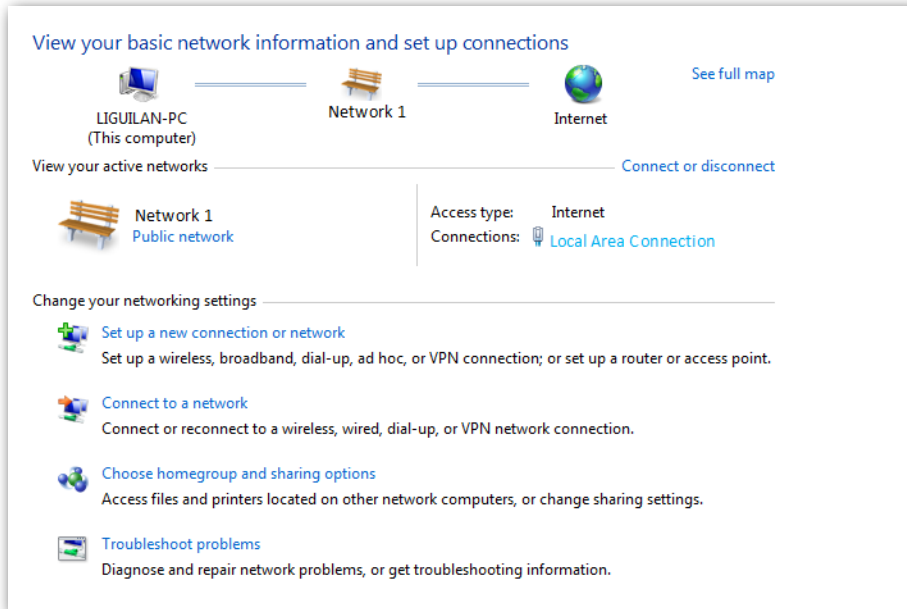
Verification

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

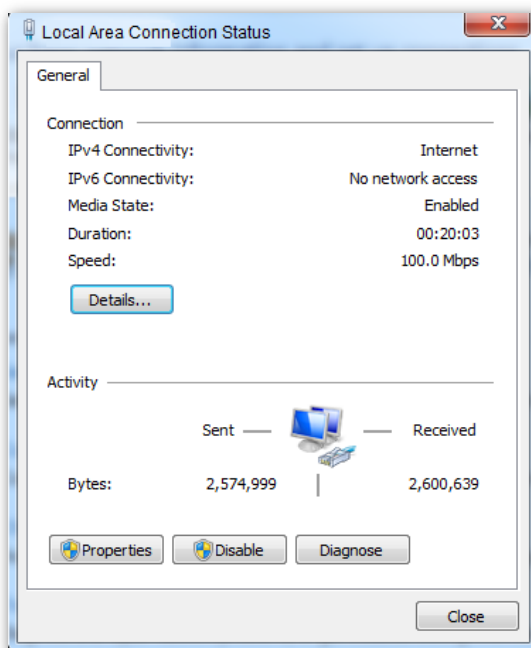
1. Right-click  in the lower-right corner of the desktop and choose **Open Network and Sharing Center**.

Open Network and Sharing Center

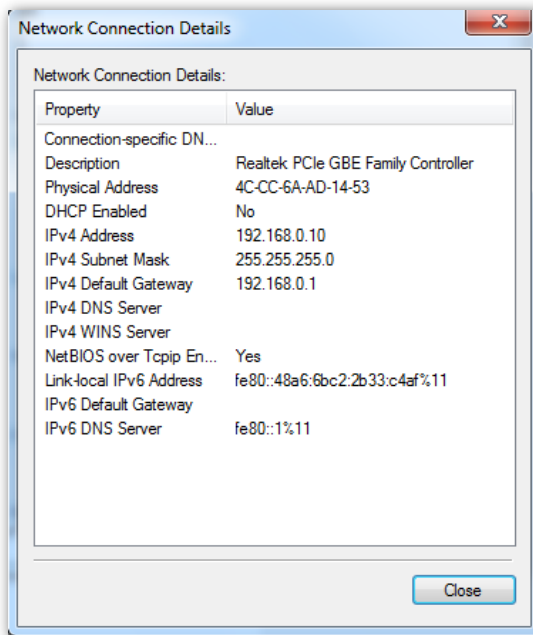
2. Click **Local Area Connection**.



3. Click **Details**.



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



Appendix B

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 and log in again:

- Ensure that all your Ethernet cables are properly connected.
- If there is no AC or IP-COM router 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 or replace your computer.
- If two or more APs are connected in the network without an AC/IP-COM management router, 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 change 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 the AC or IP-COM router in the network, 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 still persists, hold the **RESET** button down for 8 seconds to restore the AP to factory settings, and then try logging in again.

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

A2: Check the following items:

- 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.
- Ensure that the firmware versions of your AP and AC are the latest firmware versions available on www.ip-com.com.cn.
- Reset your AP.

Method to reset: When the system LED indicator blinks, hold down the **RESET** button for about 8 seconds. The AP is reset successfully when the system LED indicator gets solid on.

Appendix C

Default Parameter Values

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

Parameter		Default Value
Login	Management IP address	192.168.0.254
	Account	Administrator
		User name: admin Password: admin
	Account	User
		User name: user Password: user
Quick Setup	Working Mode	AP Mode
LAN Setup	IP Address Type	Static
	IP Address	192.168.0.254
	Subnet Mask	255.255.255.0
	Gateway	192.168.0.1
	Primary DNS Server	8.8.8.8
	Secondary DNS Server	8.8.4.4
	Device Name	Wireless Access Point
	Driving Capability of Port	Standard
DHCP Server	DHCP Server	Disable
	Start IP Address	192.168.0.100
	End IP Address	192.168.0.200
	Lease Time	1 day
	Subnet Mask	255.255.255.0
	Gateway	192.168.0.1
	Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4	
Basic Settings	SSID	The AP allows 4 SSIDs. As the primary SSID, the first SSID in the

Parameter	Default Value
	drop-down-list box is enabled by default, and the other SSIDs are disabled.
Broadcast SSID	Enable
Isolate Client	Disable
WMF	Disable
Probe Broadcast Packet Control	Disable
Max. Number of Clients	48
Chinese SSID Encoding	UTF-8
Security Mode	None
RF Status	Enable RF
	Country/Region
	Network Mode
	Channel
	Channel Bandwidth
	Extension Channel
	Lock Channel
	Transmit Power
	Lock Power
	Preamble
	Isolate SSID
	Short GI
Radio Optimizing	Beacon Interval
	Fragment Threshold
	RTS Threshold
	DTIM Interval
	Min. RSSI Threshold
	Interference Mitigation
	APSD
	Client Timeout Interval
WMM Setup	WMM
	WMM Optimization Mode
Access Control	MAC Filter Mode
Advanced	Recognize Terminal Type

Parameter	Default Value		
	Filter Broadcast Data	Disable	
QVLAN Setup		Disable	
	PVID	1	
	Management VLAN	1	
	2.4G SSID VLAN ID	1000	
SNMP	SNMP Agent	Disable	
	Administrator	Administrator	
	Device Name	Wireless Access Point	
	Location	ShenZhen	
	Read Community	public	
	Read/Write Community	private	
Deployment		Local Deployment	
Tools	Date & Time	System Time	Sync with Internet time servers is enabled: Sync Interval: 30 minutes Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei
		Login Timeout	5 minutes
	Type of Logs to Display		All
	Log server settings		None
	Time Reboot		Disable
	LED		Turn On All Indicators
	Uplink Detection		Disable
	Pinging Interval		10 minutes



CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

The mains plug is used as disconnect device, the disconnect device shall remain readily operable.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

Declaration of Conformity

Hereby, IP-COM NETWORKS Co., LTD. declares that the radio equipment type AP325 is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address:

<http://www.ip-com.com.cn/en/ce.html>

Operate Frequency: 2.4GHz: EU/2.412GHz-2.472GHz

EIRP Power (Max.): 2.4GHz: 19.9 dBm

Software Version: V1.0.0.3



FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

Operating temperature: (-10 – 45) °C

Operating humidity: (10% – 90%) RH, non-condensing



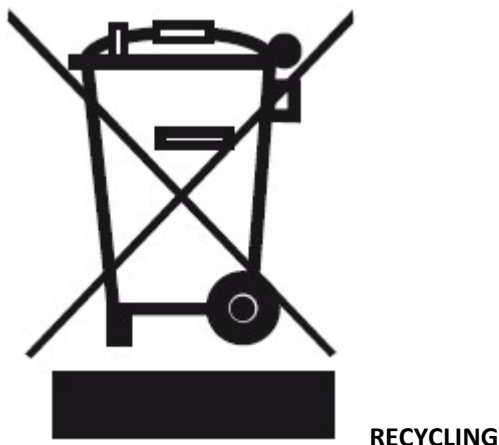
Adapter Model: BN036-A12012E/BN036-A12012B

Manufacture: SHENZHEN HEWEISHUN NETWORK TECHNOLOGY Co., LTD.

Input: 100-240 V AC, 50/60 Hz, 0.4 A

Output: 12 V DC 1 A

 : DC Voltage



This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment.

User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.



Technical Support

Telephone: (86755) 2765 3089

Email: info@ip-com.com.cn

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

Address Info:

Room 101, Unit A, First Floor, Tower E3, NO.1001, Zhongshanyuan Road, Nanshan District, Shenzhen, China.
518052

Copyright

© 2018 IP-COM Networks Co., Ltd. All rights reserved.

This documentation (including pictures, images, and product specifications, etc.) is for reference 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.