

www.ip-com.com.cn

User Guide

300 Mbps Wireless In-Wall Access Point • W30AP

IP-COM
World Wide Wireless

Copyright Statement

©2016 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 W30AP.

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

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
AP	Access Point
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMZ	Demilitarized Zone
DNS	Domain Name System
IPTV	Internet Protocol Television
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
MPPE	Microsoft Point-to-Point Encryption
PPP	Point To Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol

Acronym or Abbreviation	Full Spelling
SSID	Service Set Identifier
STB	Set Top Box
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WISP	Wireless Internet Service Provider
WPS	WiFi Protected Setup

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	Get to Know Your Device	1
1.1	Overview	1
1.2	Appearance	1
1.2.1	Button, LED Indicator, and Ports	1
1.2.2	Label.....	2
2	Application Scenarios	3
2.1	Large Apartment or Villa	3
2.1.1	Deploying the AP with an IP-COM Router that Includes the AP Controller Functionality	3
2.1.2	Deploying the AP with Another Brand’s Router.....	5
2.2	Hotel.....	8
3	Login	11
3.1	Logging in to the Web UI of the AP	11
3.2	Logging Out of the Web UI of the AP	12
3.3	Management UI Layout.....	13
3.4	Common Buttons	13
4	Quick Setup	15
4.1	Overview	15
4.2	Quick Setup	16

4.2.1 AP Mode	16
4.2.2 APClient Mode	17
5 Status	19
5.1 System Status	19
5.2 Wireless Status	20
5.3 Traffic Statistics	21
5.4 Wireless Clients	21
6 Network Settings	22
6.1 LAN Setup	22
6.2 Changing the LAN IP Address of the AP	23
6.2.1 Manually Setting the IP Address	23
6.2.2 Automatically Obtaining an IP Address	24
6.3 DHCP Server	25
6.3.1 Overview	25
6.3.2 Configuring the DHCP Server	25
6.3.3 Viewing the DHCP Client List	26
7 Wireless Settings	28
7.1 Basic Settings	28
7.1.1 Overview	28
7.1.2 Changing the Basic Settings	30
7.1.3 Examples of Configuring Basic Settings	34
7.2 Radio Status	53
7.2.1 Overview	53

7.2.2 Changing the Radio Settings	53
7.3 Channel Scan	56
7.3.1 Overview	56
7.3.2 Scanning Channels	56
7.4 WMM Settings	57
7.4.1 Overview	57
7.4.2 Changing the WMM Settings	58
7.5 Advanced.....	60
7.5.1 Overview	60
7.5.2 Changing the Advanced Settings.....	60
7.6 Access Control	62
7.6.1 Overview	62
7.6.2 Configuring Access Control	62
7.6.3 Example of Configuring Access Control	63
7.7 QVLAN	65
7.7.1 Overview	65
7.7.2 Configuring the QVLAN Function	65
7.7.3 Example of Configuring QVLAN Settings	66
8 SNMP	69
8.1 Overview	69
8.1.1 SNMP Management Framework.....	69
8.1.2 Basic SNMP Operations.....	69
8.1.3 SNMP Protocol Version	70

8.1.4 MIB Introduction	70
8.2 Configuring the SNMP Function	70
8.3 Example of Configuring the SNMP Function	72
9 Deployment	74
9.1 Overview	74
9.2 Configuring the Deployment Mode	75
9.2.1 Configuring Local Deployment Mode	75
9.2.2 Configuring Cloud Deployment Mode	75
10 Tools	77
10.1 Firmware Upgrade	77
10.2 Time & Date	78
10.2.1 System Time.....	78
10.2.2 Login Timeout.....	79
10.3 Viewing Logs	81
10.3.1 View Logs	81
10.3.2 Configuring Log Settings	82
10.4 Configuration Management.....	85
10.4.1 Backing Up and Restoring Configurations	85
10.4.2 Restoring the Factory Settings.....	85
10.5 Username and Password	87
10.6 Diagnostics Tool	88
10.7 Device Reboot.....	89
10.7.1 Device Reboot.....	89

10.7.2 Time Reboot	89
10.8 LED	91
10.9 Uplink Detection	92
10.9.1 Overview	92
10.9.2 Configuring Uplink Detection	92
Appendixes	94

1 Get to Know Your Device

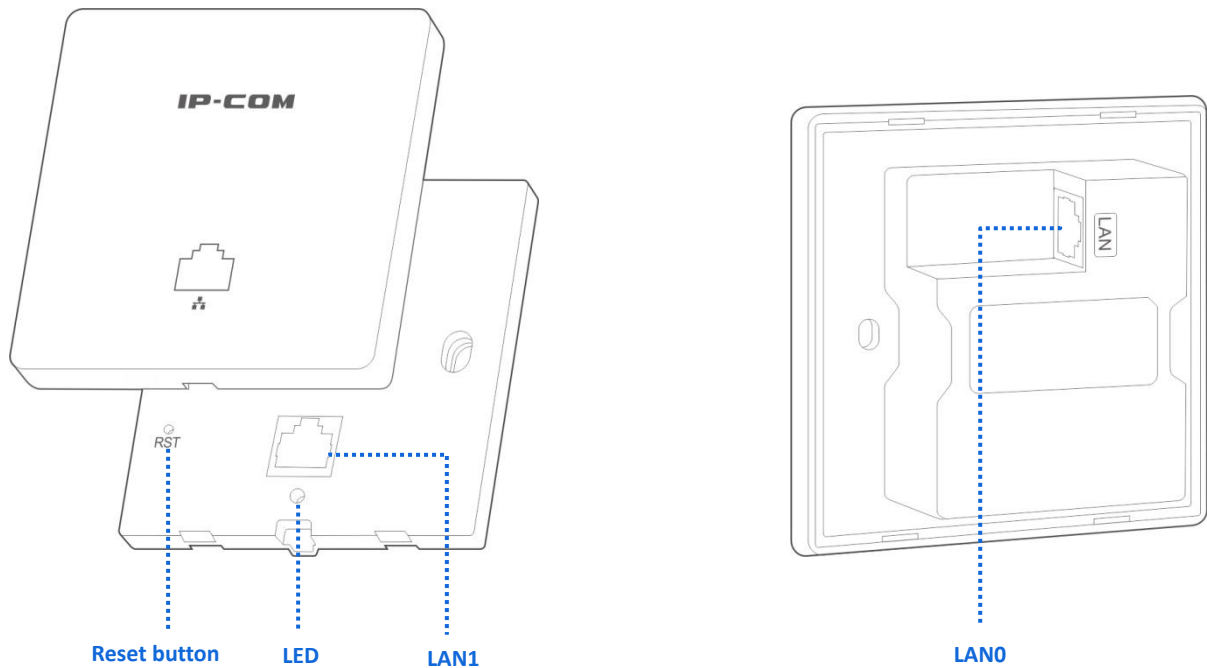
1.1 Overview

IP-COM wireless in-wall access point (AP) W30AP V4.0 offers a wireless transmission rate of as high as 300 Mbps. It can be powered through IEEE 802.3af PoE and managed using its web UI or an IP-COM wireless AC controller (or a router that includes the AP controller functionality). The in-wall design makes W30AP V4.0 perfect for providing wireless network coverage in villas, large apartments, and hotels.

1.2 Appearance

This section describes the [button, LED indicator](#), ports, and [label](#) of the AP.

1.2.1 Button, LED Indicator, and Ports



- Reset Button

It is visible after the front cover of the AP is removed. After the AP is powered on, you can use a paper clip to hold down this button for 8 seconds to restore the factory settings.

- LED Indicator

LED Indicator	Blinking: The AP is working properly.
	Off: The AP is not powered on, the indicator has been turned off, or the AP is faulty.

- LAN1 Port

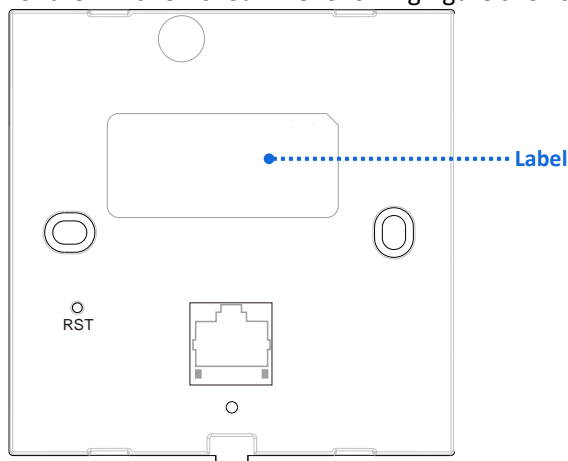
This port is located on the front panel of the AP and transmits data in 10/100 Mbps auto-negotiation mode. It is used to connect to a computer and switch and so on.

- LAN0 Port

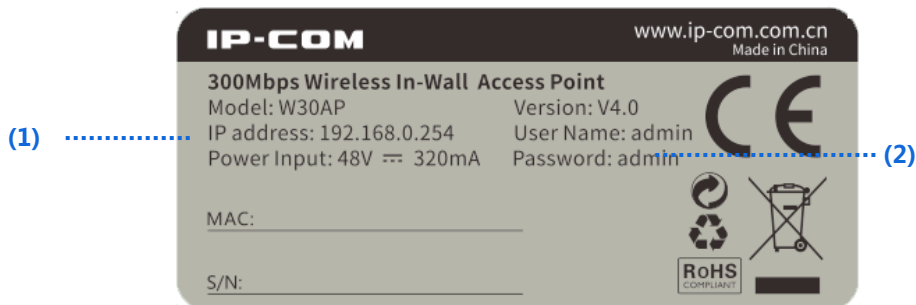
It is located on the back of the AP for supplying power to the AP through PoE and exchanging data in 10/100 Mbps auto-negotiation mode. Connect this port using an Ethernet cable to an IEEE 802.3af PoE switch or PoE power supply equipment to supply power to the AP.

1.2.2 Label

It is visible after the front cover of the AP is removed. The following figure shows its position.



The label is described as follows:



(1): Default IP address of the AP. You can use this IP address to log in to the web UI of the AP.

(2): Default user name and password of the web UI of the AP.

2 Application Scenarios

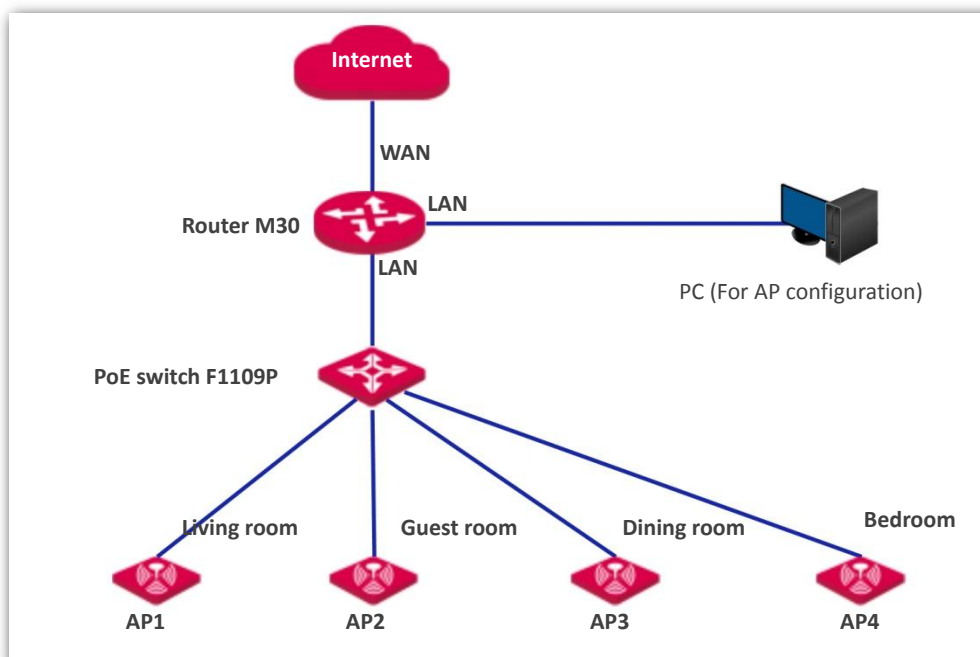
2.1 Large Apartment or Villa

2.1.1 Deploying the AP with an IP-COM Router that Includes the AP Controller Functionality

For a large apartment or villa, you are recommended to adopt the IP-COM wireless product suite, which includes a wired router (such as M30), a PoE switch (such as F1109P), and 4 to 8 W30APs. Deploy one W30AP in each room and place the router and switch in an electronic junction box. The following describes the procedure.

1. Connect the devices.

Connect the WAN port of the router to the ADSL or optical modem. Connect a LAN port of the router to the Uplink port of the PoE switch. Connect the LAN0 port of each AP to a PoE port of the switch using the in-wall Category 5 UTP cable led into each EU-type electrical wall box used to mount the APs. See the following figure.



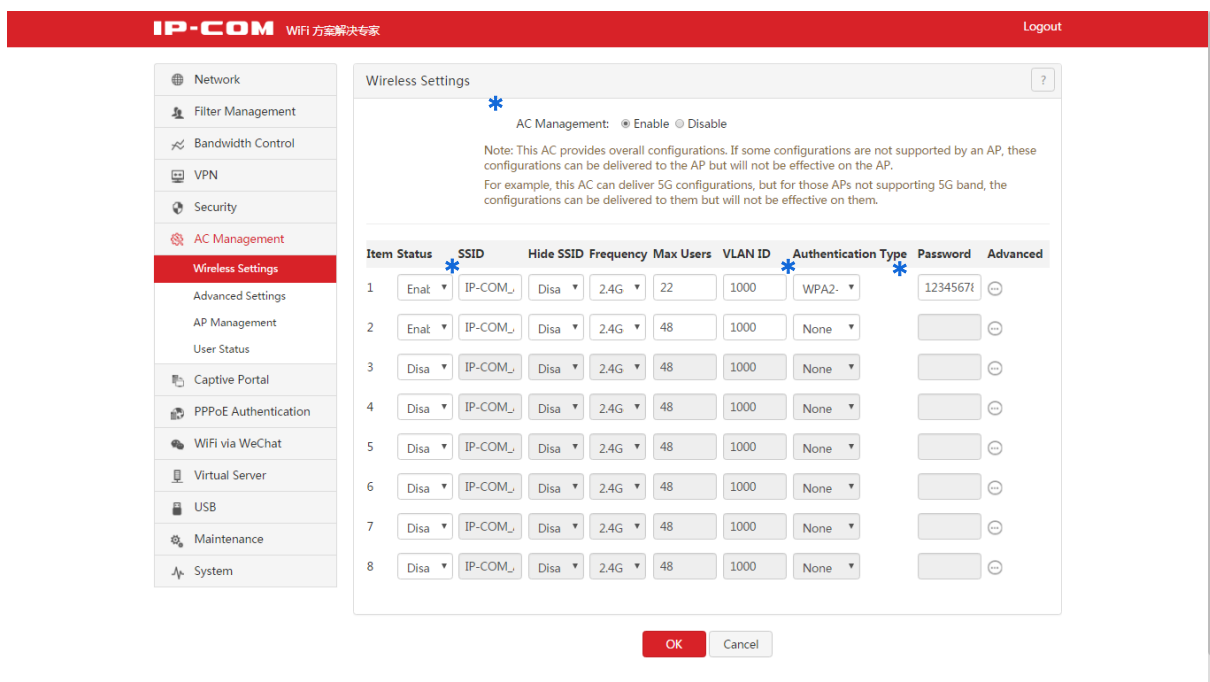
2. Log in to the web UI of the router.

Connect a computer for configuring the AP to the LAN port of the router. Start a web browser, enter the management IP address of the router (default: **192.168.0.252**), and press **Enter**. Set your password on the page that appears, and click **Login** to access the home page of the web UI.



3. Configure the AP.

Click **AC Management > Wireless Settings** to open the **Wireless Settings** module, and click **Enable**. Change the SSID (WiFi name, such as IP-COM), set the Authentication Type as **WPA2-PSK**, enter the wireless password (such as 12345678), and click **OK** to save the configuration.



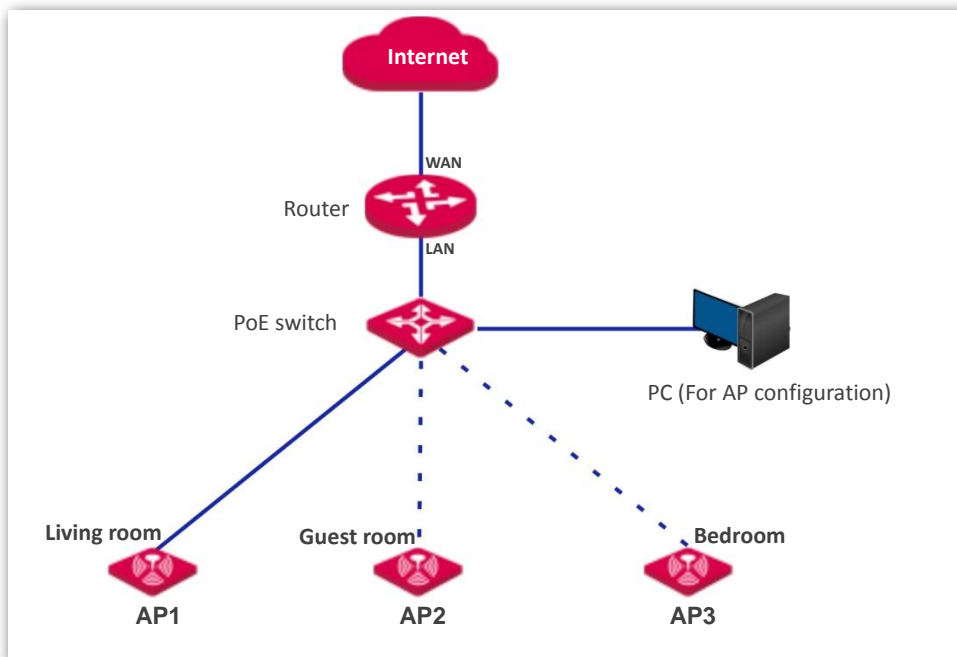
Please wait. The AP will automatically obtain the wireless network name and password from the router. For details about how to configure the AP on the router web UI, refer to the user guide for the router. The user guide is available at <http://www.ip-com.com.cn>.

2.1.2 Deploying the AP with Another Brand's Router

The following describes the procedure.

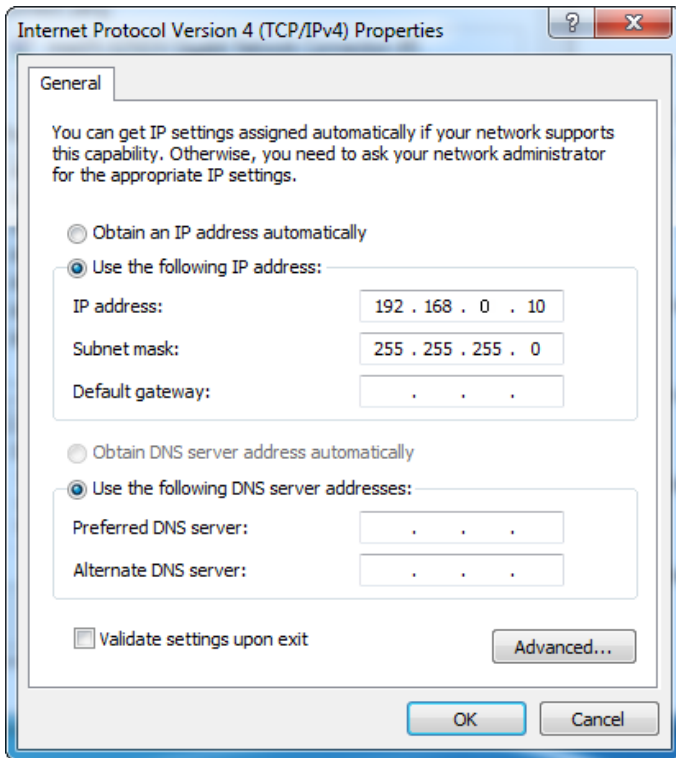
1. Connect the devices.

Connect one AP (such as AP1) to the PoE switch, as shown in the following topology. [Change the IP address of the AP](#) to prevent IP address conflicts. Repeat this procedure to configure the other APs.



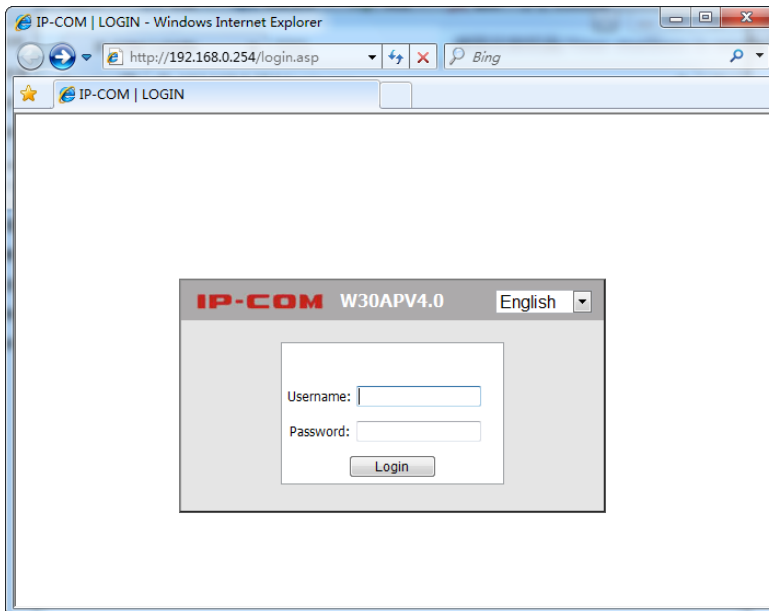
2. Set the IP Address of Your Computer (Example: Windows 7)

Use an Ethernet cable to connect the computer to the PoE switch. Right-click the network icon in the lower-right corner of the desktop of the computer, and click **Open Network and Sharing Center, Local Area Connection**, and then **Properties**. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, select **Use the following IP address**, set **IP address** to **192.168.10.X** (X: 2 - 253) and **Subnet mask** to **255.255.255.0**, and click **OK**.



3. Log in to the Web UI of the AP.

Start a web browser, enter the management IP address of the AP (default: **192.168.0.254**), and press **Enter**. Enter the user name and password of the AP (default user name and password: **admin**) and click **Login**.



4. Set AP1.

- (1) To access the page, click **Quick Setup**. Select the check box of **AP Mode**, enter an SSID (wireless network name, such as IP-COM), select **WPA2-PSK** from the dropdown list box of Security Mode, select the check box of **AES as the Cipher Type**, enter a security key (wireless network password, such as 12345678), and click **Save**.

IP-COM www.ip-com.com.cn

Quick Setup

Mode: AP Mode APClient Mode Save

SSID: IP-COM Restore

Security Mode: WPA2-PSK Help

Cipher Type: AES TKIP TKIP&AES

Security Key: 12345678

- (2) Choose **Network > LAN Setup**, change the last network segment of the IP address to prevent IP address conflicts with the later connected APs, such as 192.168.0.201, and click **Save**.

LAN Setup

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

Address Mode: Static IP Restore

IP Address: * 192.168.0.201 For example: 192.168.1.1

Subnet Mask: 255.255.255.0 For example: 255.255.255.0 Help

Gateway: 192.168.0.1

Primary DNS Server: 8.8.8.8

Secondary DNS Server (optional): 8.8.4.4

Device Name: W30APV4.0

Ethernet Mode: Auto-negotiation 10M half-duplex

5. Set the other APs.

Connect another AP to the PoE switch, refer to **Step 3 > Step 4**. It uses the same SSID and security key with but different IP address from AP1. Setting of the rest of APs can be done in the same manner.

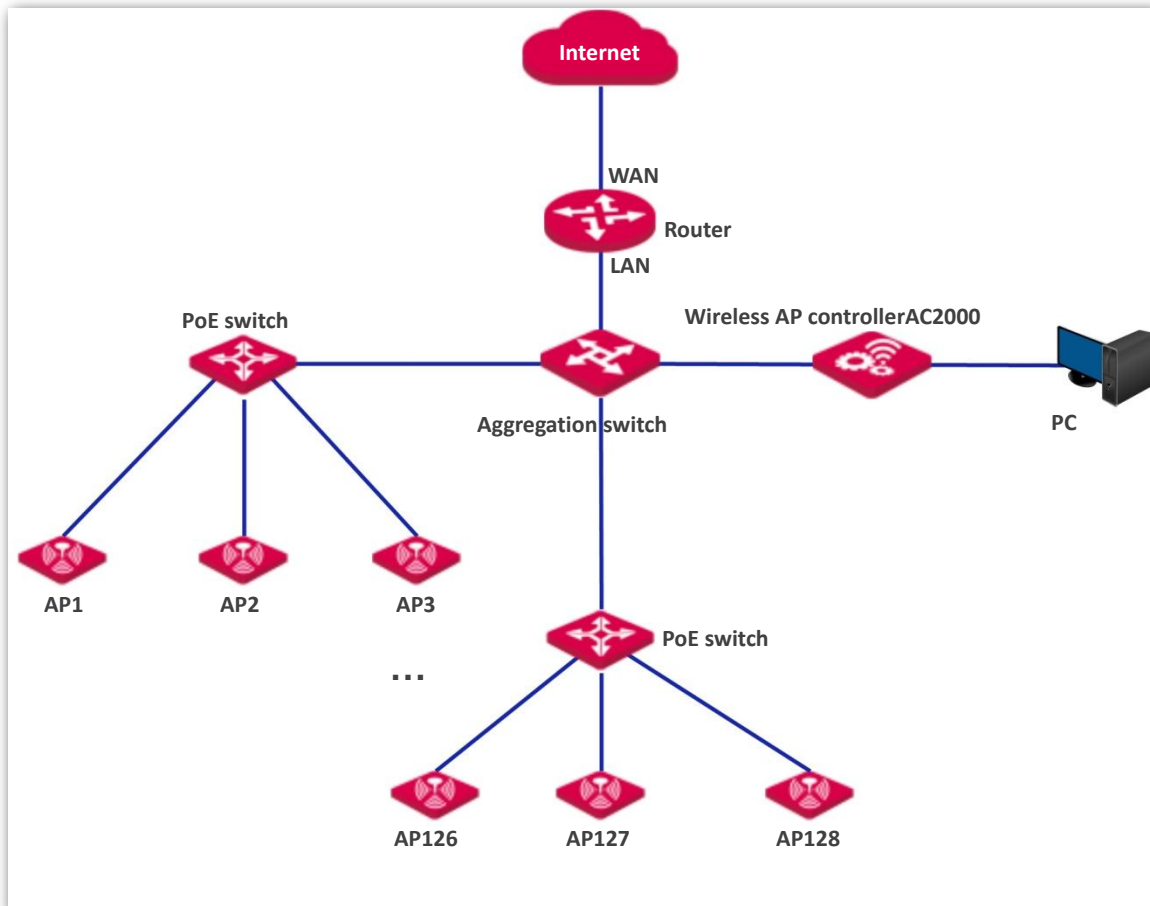
For more description of settings, please see contents from Chapter 4.

2.2 Hotel

A hotel may be deployed with a large number of APs. You can use IP-COM wireless AP controller (such as AC2000) to configure and manage them centrally and efficiently. The following describes the procedure.

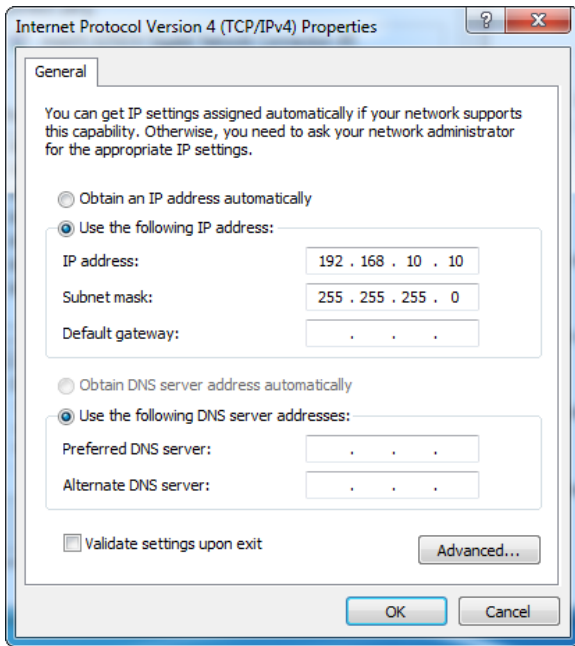
1. Connect the devices.

See the following figure.



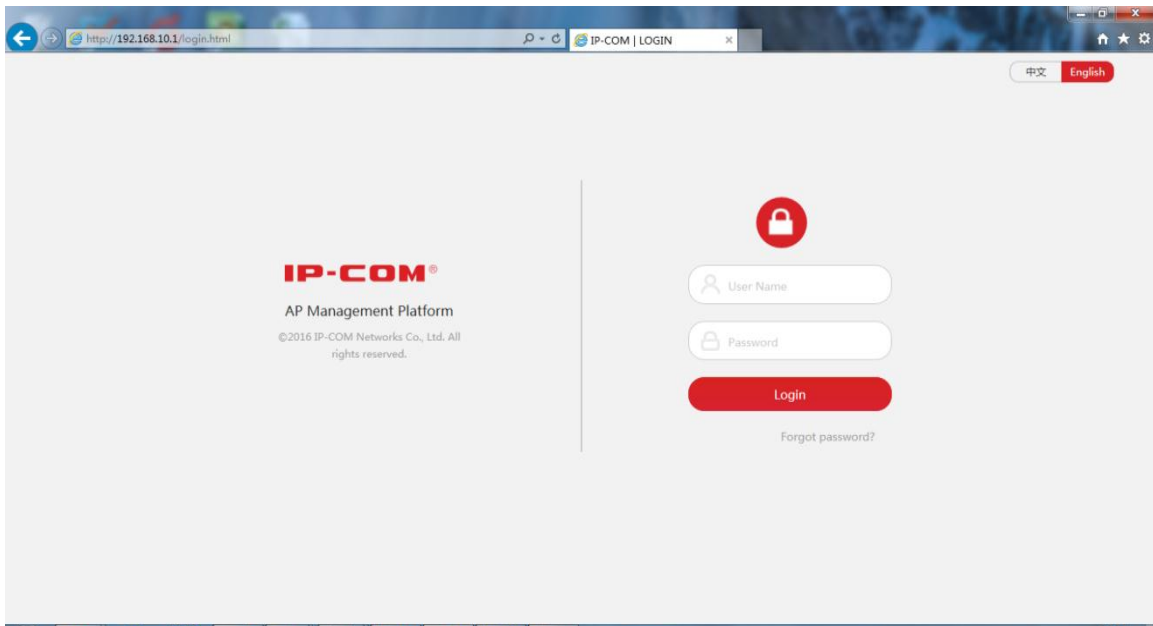
2. Set the IP Address of Your Computer (**Example: Windows 7**)

Use an Ethernet cable to connect the computer to the AP controller. Right-click the network icon in the lower-right corner of the desktop of the computer, and click **Open Network and Sharing Center, Local Area Connection**, and then **Properties**. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, select **Use the following IP address**, set **IP address** to **192.168.10.X** (X: 2~253) and **Subnet mask** to **255.255.255.0**, and click **OK**.




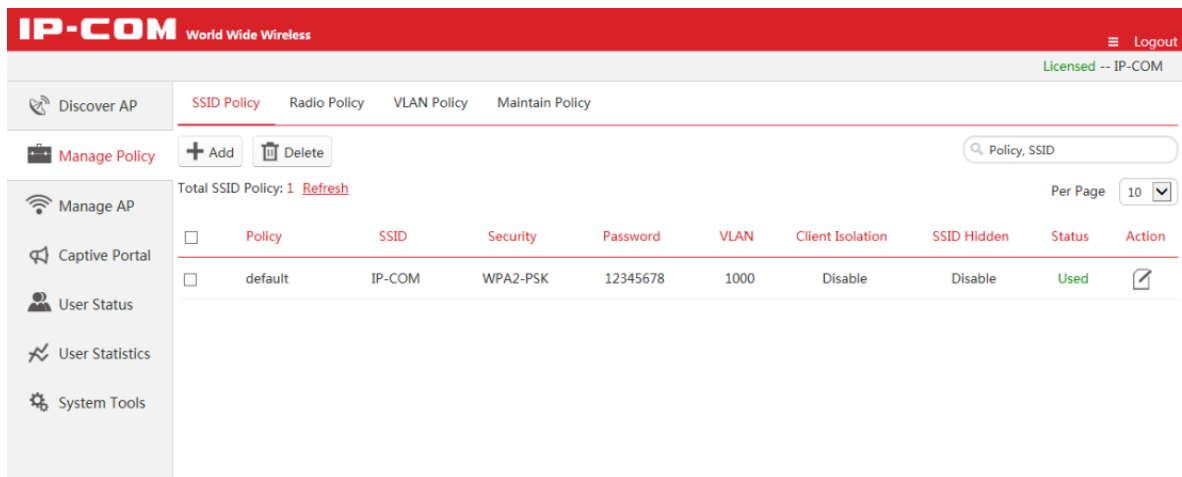
3. Log in to the web UI of the AP controller.

Start a web browser, enter the management IP address of the AP controller (default: **192.168.10.1**), and press **Enter**. Enter the user name and password of the AP controller (default user name and password: **admin**) and click **Login**.



4. Configure the APs.

To access the page, choose **Manage Policy**. Click  to change the SSID (wireless network name, such as IP-COM), Security mode (such as WPA2-PSK, AES), wireless network password (security key, such as 12345678), and save the settings.



Please wait. The AP will automatically obtain wireless network name and password from the wireless AP controller. For details about how to configure the AP on the web UI of the AP controller, visit <http://www.ip-com.com.cn> to download the user guide.

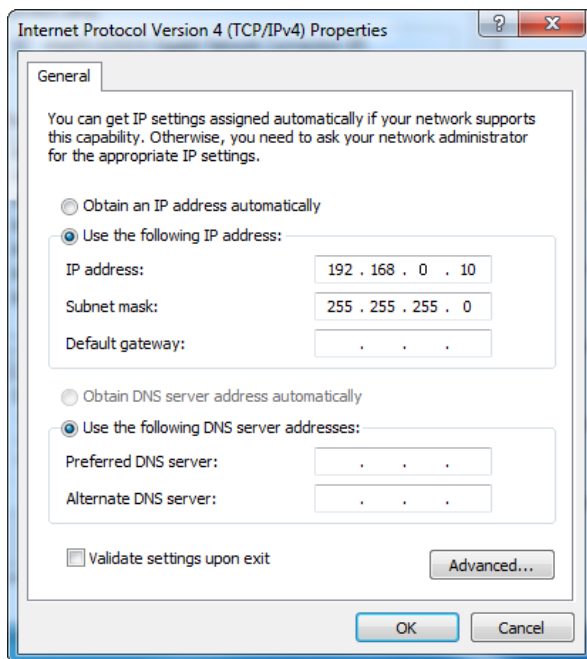
The following chapters describe how to configure the AP on the web UI of the AP.

3 Login

3.1 Logging in to the Web UI of the AP

You can log in to the web UI of the AP using a web browser. The procedure is as follows:

1. Use an Ethernet cable to connect the management computer to the AP or the switch connected to the AP.
2. Set **IP address** of your local area connection to **192.168.0.X** (X: 2 - 253) and **Subnet mask** to **255.255.255.0**.



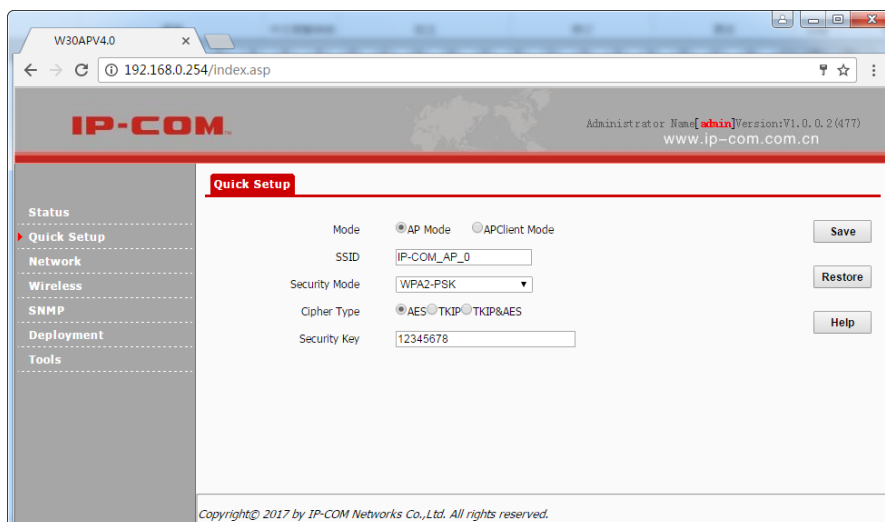
3. Start a web browser on the computer, enter the management IP address of the AP (default: 192.168.0.254) in the address bar, and press **Enter**.
4. Enter the user name and password of the AP (default user name and password: **admin**) and press **Login**.



If this page is not displayed, refer to **Q1** in **FAQ**.

---End

You can now start configuring the AP.

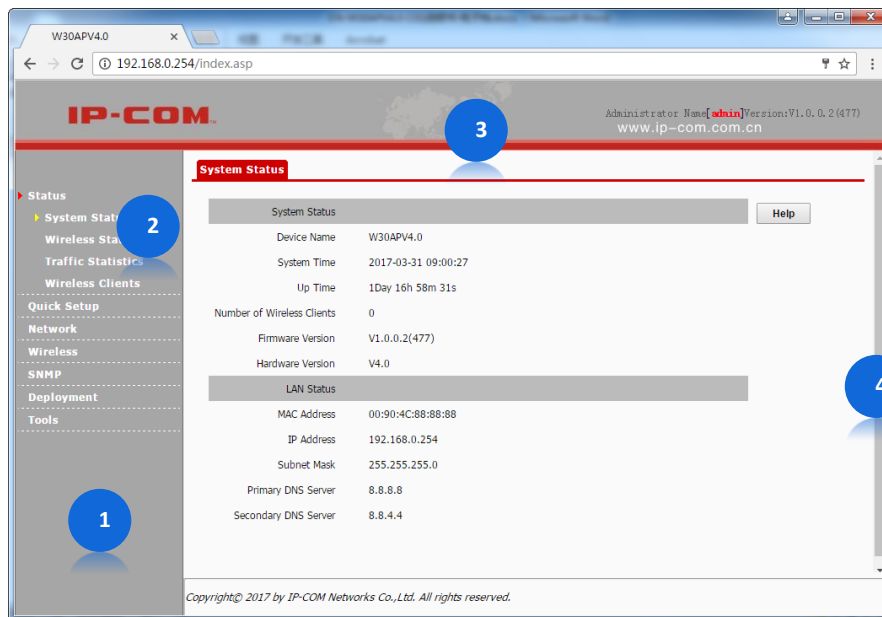


3.2 Logging out of the Web UI of the AP

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. When you close the web browser, the system logs you out as well.

3.3 Management UI Layout

The web UI of the AP is composed of three parts, including the 2-level navigation tree, tab page area, and configuration area. See the following figure.



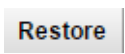

The functions and parameters dimmed on the web UI indicates that they are not supported by the AP or cannot be changed in the current configuration.

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 navigation bar, the configuration of the function appears in the configuration area.
②	Level-2 navigation bar	
③	Tab page area	
④	Configuration area	It enables you to view and modify configuration.

3.4 Common Buttons

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

Button	Description
	It is used to update the content of the current page.
	It is used to save the configuration on the current page and enable the configuration to take effect.

Button	Description
 A rectangular button with a light gray background and a thin border. The word "Restore" is written in a bold, black, sans-serif font in the center.	It is used to change the current configuration on the current page back to the original configuration.
 A rectangular button with a light gray background and a thin border. The word "Help" is written in a bold, black, sans-serif font in the center.	It is used to view help information corresponding to the settings on the current page.

4 Quick Setup

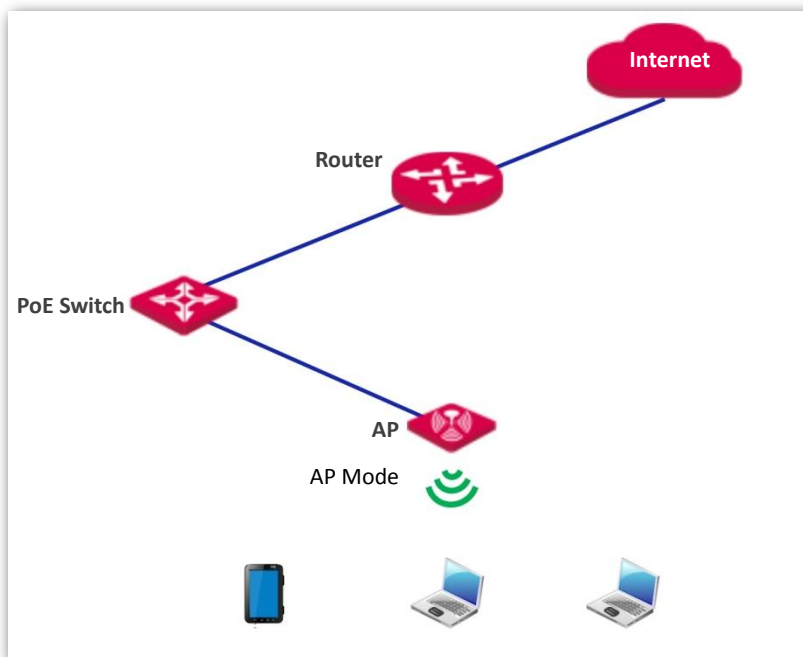
4.1 Overview

This module enables you to quickly configure the AP so that wireless devices such as smart phones and pads can access the internet through the wireless network of the AP.

This AP can work in AP or APClient mode.

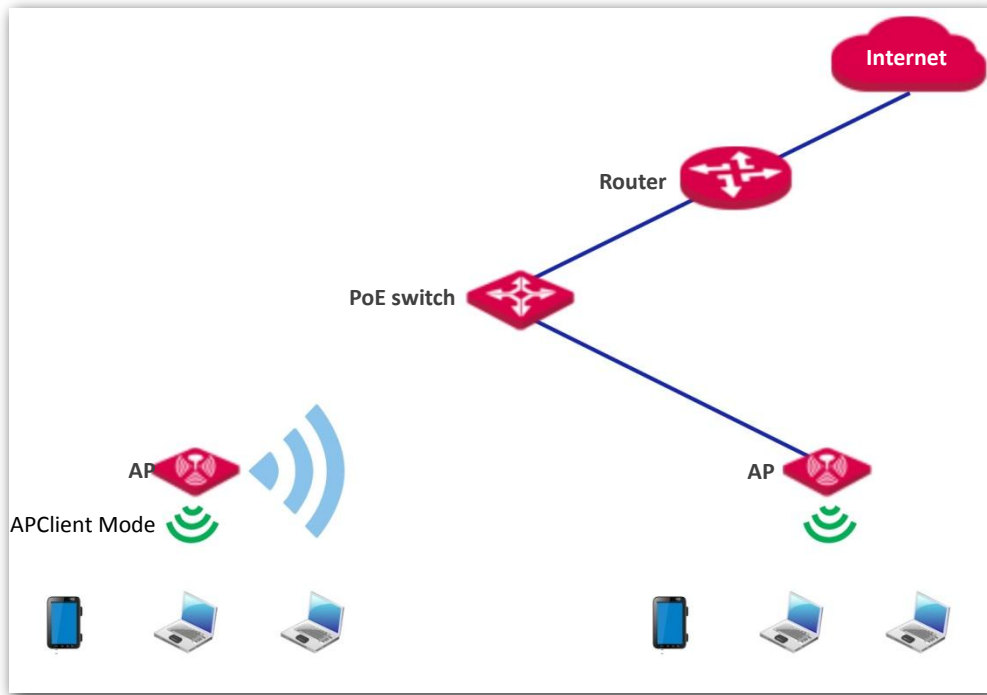
- AP Mode

By default, the AP works in this mode. In this mode, the AP connects to the internet using an Ethernet cable and converts wired signals into wireless signals to provide wireless network coverage. See the following topology.



- APClient Mode

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



4.2 Quick Setup

4.2.1 AP Mode

1. Choose **Quick Setup**.
2. Select the **AP Mode** check box.
3. (Optional) Change the value of **SSID**, which indicates the primary SSID of the AP, to your wireless network name.
4. Select a security mode from the **Security Mode** drop-down list box and set the corresponding parameters. (You are recommended to set **Security Mode** to **WPA2-PSK** and **Cipher Type** to **AES**.)
5. Click **Save**.

The screenshot shows the IP-COM Quick Setup web interface. The top header includes the IP-COM logo and the text 'Administrator Name[admin]Version:V1.0.0.2(477) www.ip-com.com.cn'. The main content area is titled 'Quick Setup' and contains the following configuration options:

- Mode:** AP Mode APClient Mode
- SSID:**
- Security Mode:**
- Cipher Type:** AES TKIP TKIP&AES
- Security Key:**

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

Parameter description

Parameter	Description
Mode	It specifies the working mode of the AP, including AP Mode and APClient Mode.
SSID	It specifies the primary SSID (wireless network name) of the AP.
Security Mode	It specifies the security mode of the wireless network of the Apothem options include: None , WEP , WPA-PSK , WPA2-PSK , Mixed WPA/WPA2-PSK , WPA , and WPA2 . Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.

---End

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

4.2.2 APClient Mode

1. Choose **Quick Setup**.
2. Set **Mode** to **APClient Mode**.
3. Click **Enable Scan**.

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

NOTE

- If no wireless network is found, choose **Wireless > Radio**, ensure that **Enable Wireless** is selected, and try scanning wireless network again.
- After a wireless network to be extended is selected, the AP identifies the SSID, security mode, and channel of the wireless network and enters them on the page. The other parameters including **Key**, **RADIUS Server IP**, **RADIUS Port**, and **RADIUS Password** must be entered manually.

Select	SSID	MAC Address	Network Mode	Channel Bandwidth	Channel	Extension Channel	Security	Signal Strength
<input type="radio"/>	IP-COM_AP_2	14:cc:20:e5:f7:31	bg	20	6	none	wpa2/tkip	-30dBm
<input type="radio"/>	IP-COM_AP_1	c8:3a:35:1f:0e:ef	bgn	20	6	none	wpa2/aes	-34dBm
<input checked="" type="radio"/>	IP-COM_AP_0	00:b0:c6:4c:0f:01	bgn	20	7	none	none	-34dBm

5. If the wireless network of the upstream device is encrypted, set **Security Key** to the wireless network password of the device or set **RADIUS Server IP**, **RADIUS Port**, and **RADIUS Password** to the IP address, port number, and password of the RADIUS server.
6. Click **Save**.

The screenshot displays the 'Quick Setup' configuration page. On the left is a navigation menu with options: Status, Quick Setup (selected), Network, Wireless, SNMP, Deployment, and Tools. The main content area is titled 'Quick Setup' and contains the following fields and controls:

- Mode:** Radio buttons for 'AP Mode' and 'APClient Mode' (selected).
- SSID:** Text input field containing 'IP-COM_AP_0'.
- Security Mode:** Dropdown menu set to 'Mixed WPA/WPA2-PSK'.
- Cipher Type:** Radio buttons for 'AES' (selected), 'TKIP', and 'TKIP&AES'.
- Security Key:** Text input field containing '12345678'.
- The Uplinked AP's channel:** Text input field containing '7'.

On the right side of the form, there are three buttons: 'Save', 'Restore', and 'Help'. At the bottom of the form, there is an 'Enable Scan' button.

---End

After the configuration, you can select the SSID (click **Status > Wireless Status** to view the SSID of this AP) on your wireless devices such as smart phones and enter your wireless network password to connect to the wireless network of the AP and access the internet through the AP. If you do not know the SSID of the AP, go to the **Wireless > Basic** page.

5 Status

5.1 System Status

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

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

The screenshot shows the 'System Status' page. On the left is a navigation menu with options: Status, System Status, Wireless Status, Traffic Statistics, Wireless Clients, Quick Setup, Network, Wireless, SNMP, Deployment, and Tools. The main content area is titled 'System Status' and contains a 'Help' button. Below the title, there are two sections: 'System Status' and 'LAN Status'. The 'System Status' section lists: Device Name (W30APV4.0), System Time (2017-03-31 09:09:57), Up Time (1Day 17h 08m 00s), Number of Wireless Clients (0), Firmware Version (V1.0.0.2(477)), and Hardware Version (V4.0). The 'LAN Status' section lists: 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), and Secondary DNS Server (8.8.4.4).

Parameter description

Parameter	Description
Device Name	It specifies the name of the AP. A unique AP name helps quickly identify the AP. You can change the AP name on the Network > LAN Setup page.
System Time	It specifies the current system time of the AP.
Up Time	It specifies the time that has elapsed since the AP was started last time.
Number of Wireless Clients	It specifies the number of wireless clients currently connected to the AP.
Firmware Version	It specifies the firmware version number of the AP.
Hardware Version	It specifies the hardware version number of the AP.
MAC Address	It specifies the physical address of the LAN port of the AP. If you connect the AP to other devices using Ethernet cables, the AP uses this MAC address to communicate with those devices.

Parameter	Description
IP Address	It specifies the IP address of the AP. The web UI of the AP is accessible at this IP address. You can change the IP address on the Network > LAN Setup page.
Subnet Mask	It specifies the subnet mask of the IP address of the AP.
Primary DNS Server	It specifies the primary DNS server of the AP.
Secondary DNS Server	It specifies the primary DNS server of the AP.

5.2 Wireless Status

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

This page displays general radio status and SSID status of the AP.

The screenshot shows the 'Wireless Status' page. On the left is a navigation menu with 'Wireless Status' highlighted. The main content area has a red header 'Wireless Status' and a 'Help' button. Below the header are two tables:

Radio Status	
Radio (On/Off)	On
Network Mode	b/g/n
Channel	8

SSID Status			
SSID	MAC Address	Working Status	Security Mode
IP-COM_AP_0	00:90:4C:88:88:89	Enabled	WPA2-PSK
IP-COM_AP_1	00:90:4C:88:88:8A	Enabled	None

Parameter description

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

5.3 Traffic Statistics

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

This page displays the statistics about historical packets of the wireless networks of the AP. To view the latest statistics, click **Refresh**.

Traffic Statistics

SSID	Total RX Traffic (MB)	Total RX Packets(Num)	Total TX Traffic (MB)	Total TX Packets(Num)
IP-COM_AP_0	50.06MB	234048	0.86MB	3457
IP-COM_AP_1	47.05MB	208025	0.77MB	3322

Help Refresh

5.4 Wireless Clients

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

This page displays information about the wireless clients connected to the wireless networks corresponding to the SSIDs of the AP.

Client List

This section displays information of connected clients (if any). Help

Host(s) Connected Currently: IP-COM_AP_0 ▼

ID	MAC Address	IP	Connection Duration	Send Speed	Receive Speed
No clients connected!					

By default, the page displays information about the wireless clients connected to the wireless network corresponding to the primary SSID of the AP. To view information about the wireless clients connected to the wireless network corresponding to the other SSID, select the SSID from the drop-down list box in the upper-right corner.

6 Network Settings

6.1 LAN Setup


To access the page, choose **Network > LAN Setup**.

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

LAN Setup

MAC Address	00:90:4C:88:88:88	<input type="button" value="Save"/>
Address Mode	Static IP ▼	<input type="button" value="Restore"/>
IP Address	<input type="text" value="192.168.0.254"/> For example: 192.168.1.1	<input type="button" value="Help"/>
Subnet Mask	<input type="text" value="255.255.255.0"/> For example: 255.255.255.0	
Gateway	<input type="text" value="192.168.0.1"/>	
Primary DNS Server	<input type="text" value="8.8.8.8"/>	
Secondary DNS Server(optional)	<input type="text" value="8.8.4.4"/>	
Device Name	<input type="text" value="W30APV4.0"/>	
Ethernet Mode	<input checked="" type="radio"/> Auto-negotiation <input type="radio"/> 10M half-duplex	

Parameter description

Parameter	Description
MAC Address	It specifies the MAC address of the LAN port of the AP. The default primary SSID of the AP is IP-COM_XXXXXX, where XXXXXX indicates the last 6 characters of this MAC address.
Address Mode	It specifies the IP address obtaining mode of the AP. The default option is Static . Static IP: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is set manually. Dynamic IP: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is obtained from a DHCP server on your LAN.  TIP If Address Mode is set to Dynamic IP , you can log in to the web UI of the AP only with the IP address assigned to the AP by the DHCP server. The IP address is specified on the client list of the DHCP server.
IP Address	It specifies the IP address of the AP. The web UI of the AP is accessible at this IP

Parameter	Description
	address. The default IP address is 192.168.0.254. Generally, ensure that this IP address is in the same network segment as the LAN IP address of your LAN router connected to the internet, so that the AP can access the internet.
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, set the gateway IP address to the LAN IP address of your LAN router connected to the internet, so that the AP can access the internet.
Primary DNS Server	It specifies the primary DNS server of the AP. If your LAN router connected to the internet provides the DNS proxy function, this IP address can be the LAN IP address of the router. Otherwise, enter a correct DNS server IP address.
Secondary DNS Server (optional)	It specifies the IP address of the secondary DNS server of the AP. This parameter is optional. If a DNS server IP address in addition to the IP address of the primary DNS server is available, enter the additional IP address in this field.
Device Name	It specifies the name of the AP. By default, the name is the model of the AP, such as W30APV4.0. You are recommended to change the name of the AP to indicate the location of the AP (such as Bedroom), so that you can easily identify the AP when managing many APs.
Ethernet Mode	It specifies the Ethernet mode of LAN0 of this AP. Auto-negotiation: This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended. 10M half-duplex: This mode features a long transmission distance but relatively low transmission rate (usually 10 Mbps). This mode is recommended only if the Ethernet cable that connects the LAN0 port of the AP to a peer device exceeds 100 meters. In this case, the connected LAN port of the peer device must work in auto-negotiation mode. Otherwise, the LAN0 port of the AP may not be able to properly transmit or receive data.

6.2 Changing the LAN IP Address of the AP

6.2.1 Manually Setting the IP Address

In this mode, you must manually set the IP address, subnet mask, gateway IP address, and DNS server IP addresses of the AP. Therefore, this mode is recommended if you need to deploy only a few APs.

Procedure:

1. Choose **Network > LAN Setup**.
2. Set **Address Mode** to **Static IP**.

3. Set **IP Address**, **Subnet Mask**, **Gateway**, and **Primary DNS Server**. If another DNS server is available, set **Secondary DNS Server** to the IP address of the additional DNS server.
4. Click **Save**.

The screenshot shows the 'LAN Setup' configuration page. The 'Address Mode' is set to 'Static IP'. The 'IP Address' field contains '192.168.0.254' with a hint 'For example: 192.168.1.1'. The 'Subnet Mask' field contains '255.255.255.0' with a hint 'For example: 255.255.255.0'. The 'Gateway' field contains '192.168.0.1'. The 'Primary DNS Server' field contains '8.8.8.8'. The 'Secondary DNS Server(optional)' field contains '8.8.4.4'. The 'Device Name' field contains 'W30APV4.0'. The 'Ethernet Mode' is set to 'Auto-negotiation' (selected) and '10M half-duplex'. There are 'Save', 'Restore', and 'Help' buttons on the right side.

---End

After the configuration, if the new and original IP addresses belong to the same network segment, you can log in to the web UI of the AP by accessing the new IP address. Otherwise, assign your computer an IP address that belongs to the same network segment as the new IP address of the AP before login.

6.2.2 Automatically Obtaining an IP Address

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

Procedure:

1. Choose **Network > LAN Setup**.
2. Set **Address Mode** to **Dynamic IP**.
3. Click **Save**.

The screenshot shows the 'LAN Setup' configuration page. The 'Address Mode' is set to 'Dynamic IP'. The 'Device Name' field contains 'W30APV4.0'. The 'Ethernet Mode' is set to 'Auto-negotiation' (selected) and '10M half-duplex'. There are 'Save', 'Restore', and 'Help' buttons on the right side.

---End

After the configuration, if you want to relog in to the web UI of the AP, check the client list of the DHCP server for the IP address assigned to the AP, ensure that the IP address of the management computer and the IP address of the AP belong to the same network segment, and access the IP address of the AP.

6.3 DHCP Server

6.3.1 Overview

The AP provides a DHCP server function to assign IP addresses to clients on the LAN. By default, the DHCP server function is disabled.



If the new and original IP addresses of the LAN port belong to different network segment, the system changes the IP address pool of the DHCP server function of the AP so that the IP address pool and the new IP address of the LAN port belong to the same network segment.

6.3.2 Configuring the DHCP Server




1. Choose **Network > DHCP Server**.
2. Set the parameters. Generally, you need to set only **DHCP Server**, **Gateway**, and **Primary DNS Server**.
3. Click **Save**.

A screenshot of a web interface for configuring the DHCP Server. The page has two tabs: "DHCP Server" (selected) and "DHCP Client List". The configuration area contains several fields: "DHCP Server" with an "Enable" checkbox (unchecked), "Start IP" (192.168.0.100), "End IP" (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(optional)" (8.8.4.4). On the right side, there are three buttons: "Save", "Restore", and "Help".

DHCP Server	
* DHCP Server	<input type="checkbox"/> Enable
Start IP	192.168.0.100
End IP	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(optional)	8.8.4.4

---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	It specifies the start IP address of the IP address pool of the DHCP server. The default value is 192.168.0.100 .
End IP	It specifies the end IP address of the IP address pool of the DHCP server. 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 address of the LAN port of the AP.
Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a client. When half of the lease time has elapsed, the client sends a DHCP Request to the DHCP server to renew the lease time. If the request succeeds, the lease time is extended according to the request. Otherwise, the client sends the request again when 7/8 of the lease time has elapsed. If the request succeeds, the lease time is extended according to the request. Otherwise, the client must request an IP address from the DHCP server after the lease time expires. It is recommended that you retain the default value 1 day .
Subnet Mask	It specifies the subnet mask assigned by the DHCP server to clients. The default value is 255.255.255.0 .
Gateway	It specifies the default IP address gateway assigned by the DHCP server to clients. Generally, it is the IP address of the LAN port of a router on the LAN. The default value is 192.168.0.254 .  TIP A client can access a server or host not in the local network segment only through a gateway.
Primary DNS Server	It specifies the primary DNS server IP address assigned by the DHCP server to clients. The default value is 192.168.0.254 .  TIP To enable clients to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS Server (optional)	It specifies the secondary DNS server IP address assigned by the DHCP server to clients. This parameter is optional.



If another DHCP server is available on 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.

6.3.3 Viewing the DHCP Client List

If the AP functions as a DHCP server, you can view the DHCP client list to understand the details about the

clients that obtain IP addresses from the DHCP server. The details include host names, IP addresses, MAC addresses, and lease times.

To access the page, choose **Network** > **DHCP Server** and click **DHCP Client List** tab.

DHCP Server **DHCP Client List**

Once DHCP is enabled, client list will be refreshed automatically every five seconds. [Refresh](#)

ID	Hostname	IP Address	MAC Address	Lease Time
1	iPad	192.168.0.150	04:52:f3:83:fc:66	23:58:27
2	android-91288d56e18039d1	192.168.0.135	a0:8d:16:42:43:21	23:59:23

To view the latest DHCP client list, click **Refresh**.

7 Wireless Settings

7.1 Basic Settings

7.1.1 Overview

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

Broadcast SSID

When the AP broadcasts an SSID, nearby wireless clients can detect the SSID. When this parameter is set to **Disable**, the AP does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. This to some extent enhances the security of the wireless network.

It is worth noting that after **Broadcast SSID** is set to **Disable**, a hacker can still connect to the corresponding wireless network if he/she manages to obtain the SSID by other means.

AP Isolation

This parameter implements a function similar to the VLAN function for wired networks. It isolates the wireless clients connected to the same wireless network corresponding to an SSID, so that the wireless clients can access only the wired network connected to the AP. Applying this function to hotspot setup at public places such as hotels and airports helps increase network security.

WMF

The number of wireless clients 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 to effectively reduce bandwidth requirements and prevent network congestion.

Nevertheless, if a large number of clients are connected to a wireless interface of a wireless network and multicast data is intended for only one of the clients, the data is still sent to all the clients, which unnecessarily increases wireless resource usage and may lead to wireless channel congestion. In addition, multicast stream forwarding over an 802.11 network is not secure.

The WMF function of the AP converts multicast traffic into unicast traffic and forwards the traffic to the

multicast traffic destination in the wireless network. This helps save wireless resources, ensure reliable transmission, and reduce delays.

Max. Number of Clients

This parameter specifies the maximum number of clients that can connect to the wireless network corresponding to an SSID. If the number is reached, the wireless network rejects new connection requests from clients. This limit helps balance load among APs.

Security Mode

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

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

- None

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

- WEP

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

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

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

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

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

7.1.2 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 change the **Enable**, **SSID**, and **Security Mode** settings.
4. Click **Save**.


The screenshot shows the 'Basic' configuration page for an SSID. The settings are as follows:

- SSID:** IP-COM_AP_0
- Enable:**
- Broadcast SSID:** Enable
- AP isolation:** Disable Enable
- WMF:** Disable Enable
- Maximum clients:** 22 (Range:1-64)
- SSID:** IP-COM_AP_0
- Chinese SSID Encode:** UTF-8
- Security Mode:** None

Buttons on the right: Save, Restore, Help.

---End

Parameter description

Parameter	Description
SSID	It specifies the SSID to be configured. The AP supports 2 SSIDs and the first SSID displayed is the primary SSID.
Enable	It specifies whether to enable the selected SSID. By default, the primary SSID is enabled. While the other SSIDs are disabled. Users can enable them if needed.
Broadcast SSID	It specifies whether to broadcast the selected SSID. <ul style="list-style-type: none">■ Enable: It indicates that the AP broadcasts the selected SSID. In this case, nearby wireless clients can detect the SSID.■ Disable: It indicates that the AP does not broadcast the selected SSID. In this case, if you want to connect a wireless client to the wireless network corresponding to the SSID, you must manually enter the SSID on the client. <p> TIP</p> <p>This AP can automatically hide its SSID. When the number of clients connected to the AP with an SSID of the AP reaches the upper limit, the AP stops broadcasting the SSID.</p>
AP Isolation	<ul style="list-style-type: none">■ Enable: It indicates that the wireless clients connected to the AP with the selected SSID cannot communicate with each other. This improves wireless network security.■ Disable: It indicates that the wireless clients connected to the AP with the selected SSID can communicate with each other. By default, it is disabled.

Parameter	Description
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.
Max. Number of Clients	<p>It specifies the maximum number of clients that can be concurrently connected to the wireless network corresponding to an SSID.</p> <p>After this upper limit is reached, the AP rejects new requests from clients for connecting to the wireless network.</p> <p>A total of 128 wireless clients are allowed for all the enabled SSIDs of the AP.</p>
SSID	<p>It enables you to change the selected SSID.</p> <p>Chinese characters are allowed in an SSID.</p>
Chinese SSID Encoding	<p>It specifies the encoding format of Chinese characters in an SSID. This parameter takes effect only if the SSID contains Chinese characters. The default value is UTF-8.</p> <p>If both SSIDs of the AP are enabled and contain Chinese characters, you are recommended to set this parameter to UTF-8 for one SSID and to GB2312 for the other, so that any wireless client can identify one or both SSIDs.</p>
Security Mode	<p>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. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.</p>

- None

It allows any wireless client to connect to a wireless network. This option is not recommended because it affects network security.

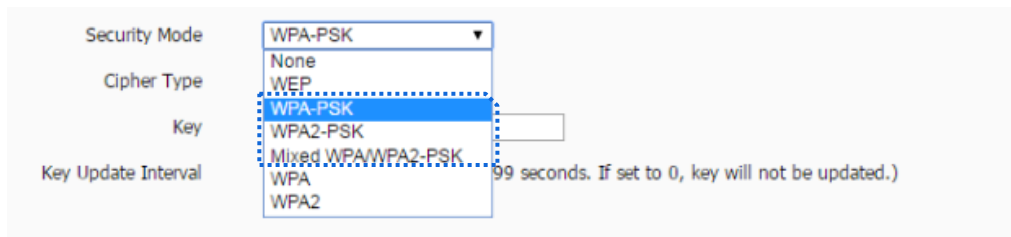
- WEP

Parameter description

Parameter	Description
Encryption Type	<p>It specifies the authentication type for the WEP security mode. The options include Open, Shared, and 802.1x. The options share the same encryption process.</p> <ul style="list-style-type: none"> ■ Open: It specifies that authentication is not required and data exchanged is encrypted using WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. ■ Shared: It specifies that a shared key is used for authentication and data exchanged is encrypted using WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key. ■ 802.1x specifies that 802.1x authentication is required and data exchanged is encrypted

Parameter	Description
	using WEP. In this case, ports are enabled for user authentication when valid clients connect to the wireless network corresponding to the selected SSID, and disabled when invalid users connect to the wireless network.
Default Key	It specifies the WEP key for the Open or Shared encryption type. For example, if Default Key is set to Security Key 2 , a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Security Key 2 .
ASCII	It indicates that a key selected for the Open or Shared authentication type contains hexadecimal characters. 5 or 13 ASCII characters are allowed in the key.
Hex	It indicates that a key selected for the Open or Shared authentication type contains hexadecimal characters. 10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key.
RADIUS Server IP	These parameters are dedicated to the 802.1x authentication type. It specifies the IP address/port number/shared key of the RADIUS server for authentication.
RADIUS Port	
RADIUS Password	

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

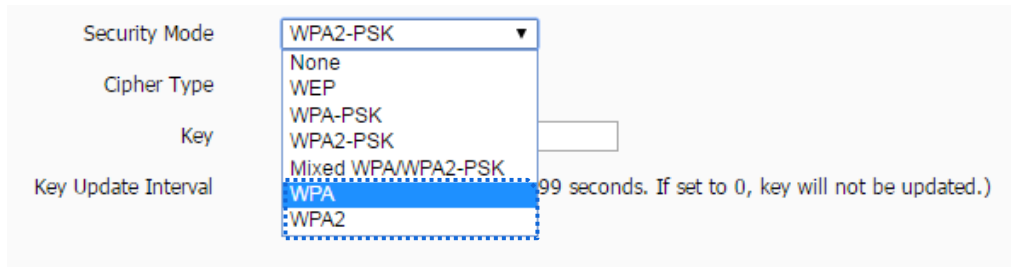


Parameter description

Parameter	Description
Security Mode	It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. <ul style="list-style-type: none"> ■ WPA-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA-PSK. ■ WPA2-PSK: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA2-PSK. ■ Mixed WPA/WPA2-PSK: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK.
Cipher Type	It specifies the encryption algorithm corresponding to the selected security mode. If Security Mode is set to WPA-PSK , this parameter has the AES and TKIP values. If Security Mode is set to WPA2-PSK or Mixed WPA/WPA2-PSK , this parameter has the AES , TKIP , and TKIP&AES values. <ul style="list-style-type: none"> ■ AES: It indicates the Advanced Encryption Standard. ■ TKIP: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. ■ TKIP&AES: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.

Parameter	Description
Key	It specifies a pre-shared WPA key. A WPA key can contain 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value 0 indicates that a WAP key is not updated.

■ WPA and WPA2



Parameter description

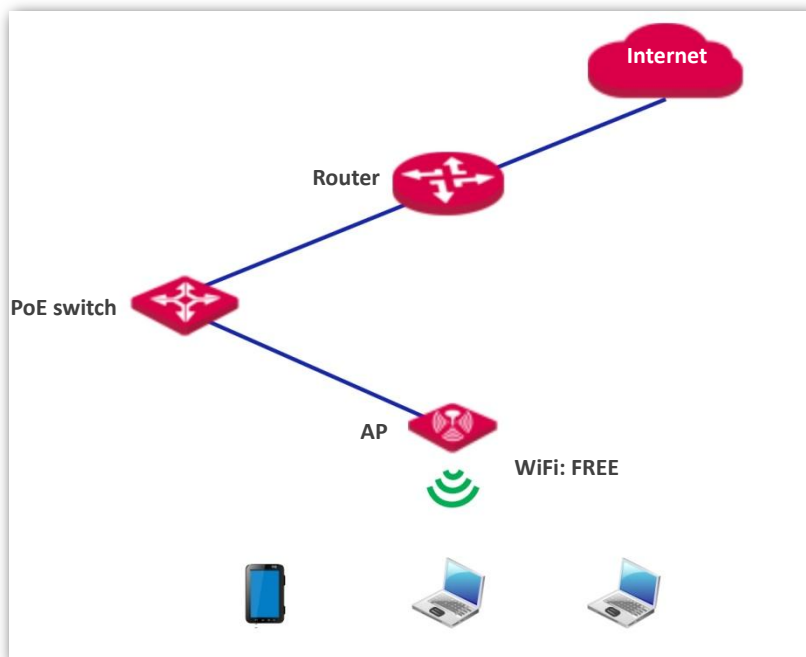
Parameter	Description
Security Mode	<p>The WPA and WPA2 options are available for network protection with a RADIUS server.</p> <ul style="list-style-type: none"> ■ WPA: It indicates that the wireless network corresponding to the selected SSID is encrypted using WPA. ■ WPA: It indicates that the wireless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

7.1.3 Examples of Configuring Basic Settings

Setting up a Non-encrypted Wireless Network

Networking requirement

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



Configuration procedure

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.
3. Select the **Enable** check box.
4. Change the value of the **SSID** text box to **FREE**.
5. Set **Security Mode** to **None**.
6. Click **Save**.

Basic

* SSID	IP-COM_AP_1	Save
* Enable	<input checked="" type="checkbox"/>	
Broadcast SSID	Enable	
AP isolation	<input type="radio"/> Disable <input type="radio"/> Enable	Help
WMF	<input type="radio"/> Disable <input type="radio"/> Enable	
Maximum clients	48 (Range:1-64)	
* SSID	FREE	
Chinese SSID Encode	UTF-8	
* Security Mode	None	

---End

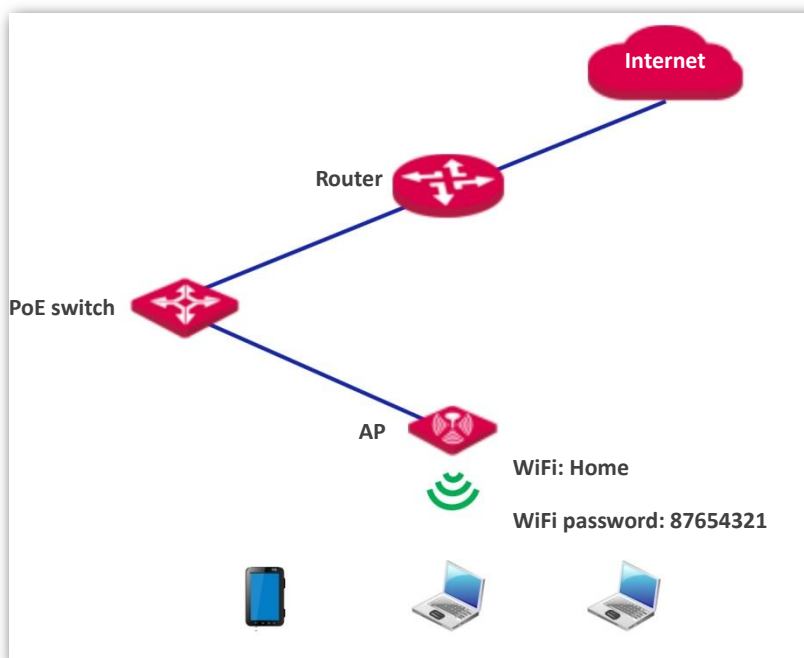
Verification

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

Setting up a Wireless Network Encrypted Using WPA/WPA2-PSK

Networking requirement

A home wireless network with a certain level of security must be set up through a simply procedure. In this case, WPA/WPA2 pre-shared key mode is recommended. See the following figure.



Configuration procedure

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

1. Choose **Wireless > Basic**.

2. Select the second SSID from the **SSID** drop-down list box.
3. Select the **Enable** check box.
4. Change the value of the **SSID** text box to **Home**.
5. Set **Security Mode** to **WPA2-PSK** and **Cipher Type** to **AES**.
6. Set **Key** to **87654321**.
7. Click **Save**.

Basic

* SSID	IP-COM_AP_1 ▾	Save
* Enable	<input checked="" type="checkbox"/>	Restore
Broadcast SSID	Enable ▾	Help
AP isolation	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
WMF	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Maximum clients	48 (Range:1-64)	
* SSID	HOME	
Chinese SSID Encode	UTF-8 ▾	
* Security Mode	WPA2-PSK ▾	
* Cipher Type	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP&AES	
* Key	87654321	
Key Update Interval	0 s (Range: 60—99999 seconds. If set to 0, key will not be updated.)	

---End

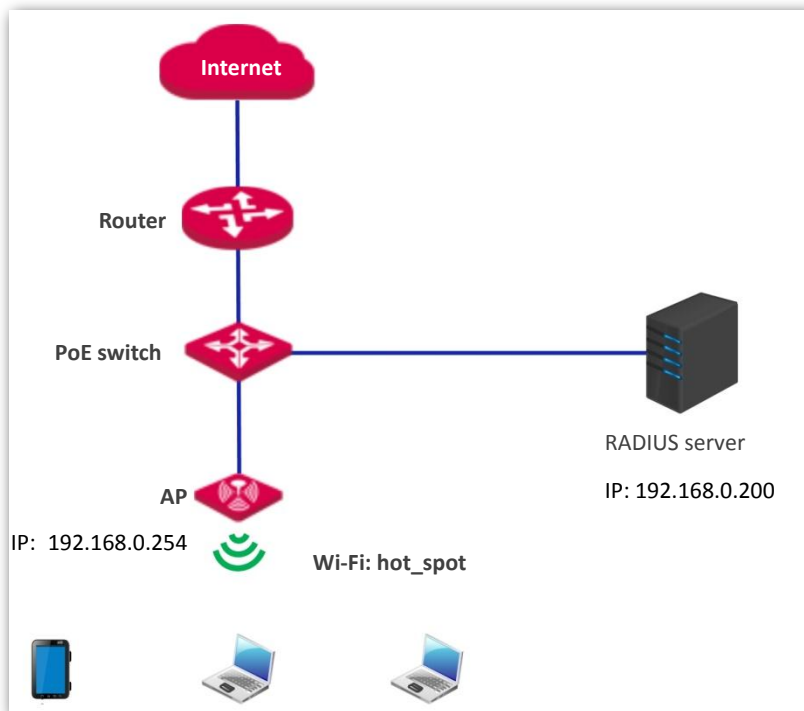
Verification

Verify that wireless devices can connect to the **Home** wireless network with the password **87654321**.

Setting up a Wireless Network Encrypted Using WPA or WPA2

Networking requirement

A highly secure wireless network is required and a RADIUS server is available. In this case, WPA or WPA2 pre-shared key mode is recommended. See the following figure.



Configuration procedure

Configure the AP.

Assume that the IP address of the RADIUS server is 192.168.0.200, the Key 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. Select the **Enable** check 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. Set **Cipher Type** to **AES**.
8. Click **Save**.

Basic

* SSID: IP-COM_AP_1

* Enable:

Broadcast SSID: Enable

AP isolation: Disable Enable

WMF: Disable Enable

Maximum clients: 48 (Range:1-64)

* SSID: hot_spot

Chinese SSID Encode: UTF-8

* Security Mode: WPA2

* RADIUS Server: 192.168.0.200

* RADIUS Port: 1812 (Range: 1025-65535,default: 1812)

* RADIUS Password: [masked]

* Cipher Type: AES TKIP TKIP&AES

Key Update Interval: 0 s (Range: 60—99999 seconds. If set to 0, key will not be updated.)

Save Restore Help

---End

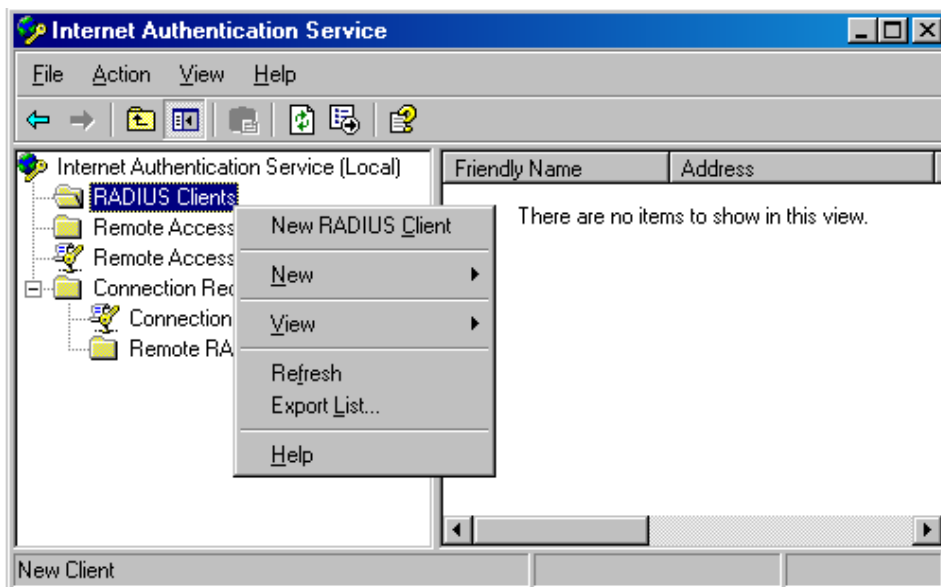
Configure the RADIUS server.



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:

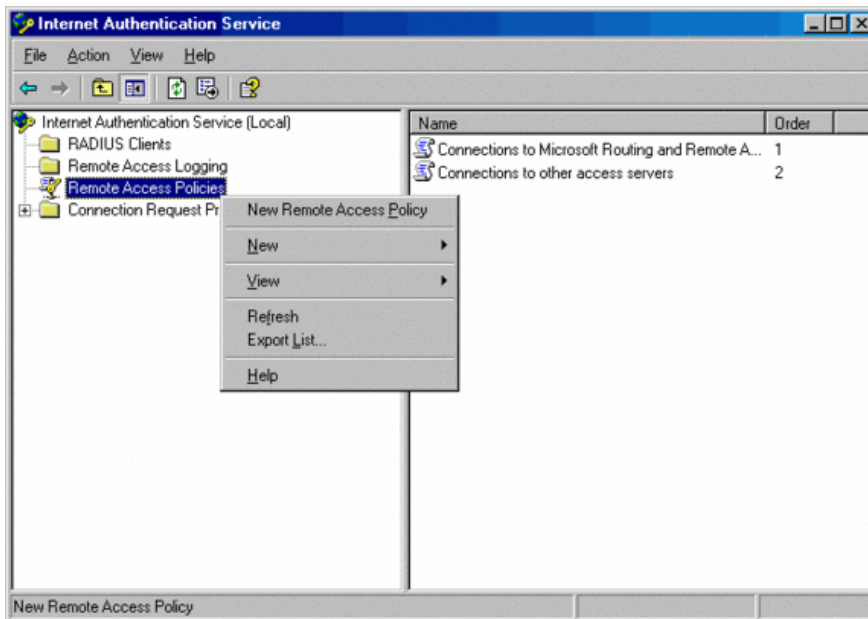
Request must contain the Message Authenticator attribute

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

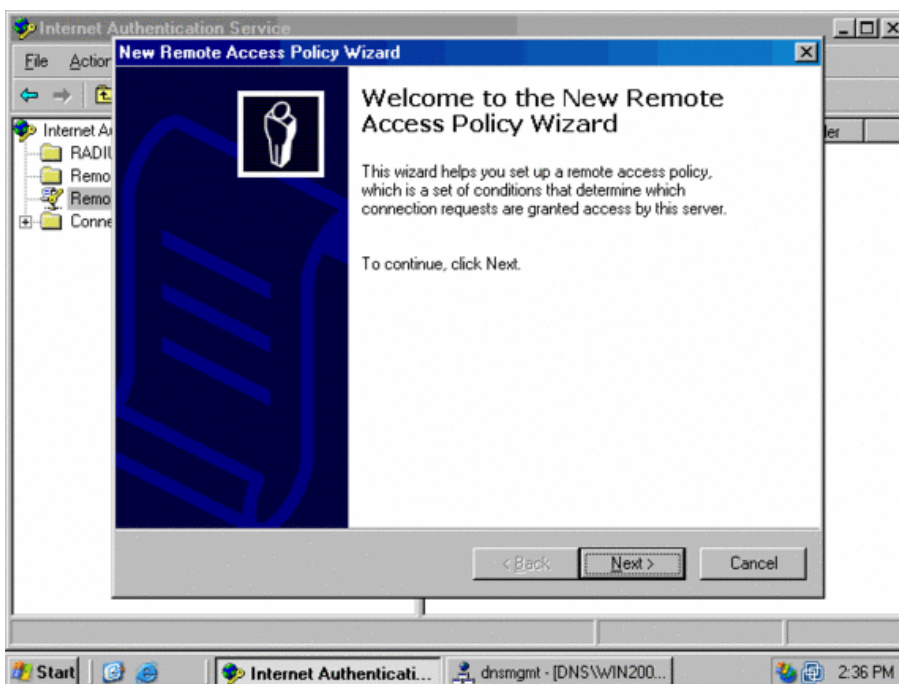
< Back Finish Cancel

2. Configure a remote access policy.

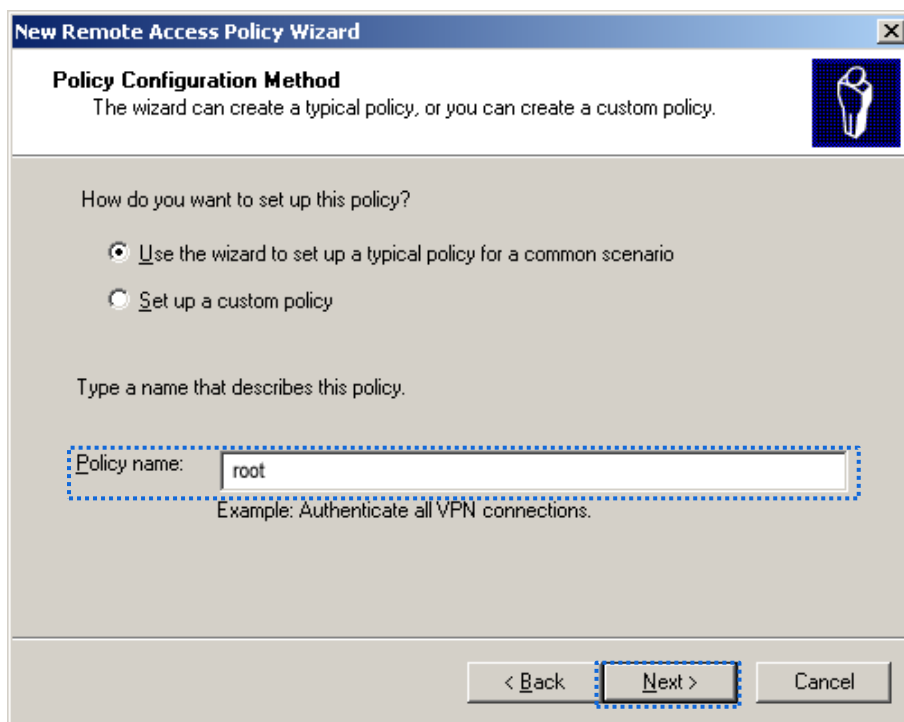
Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



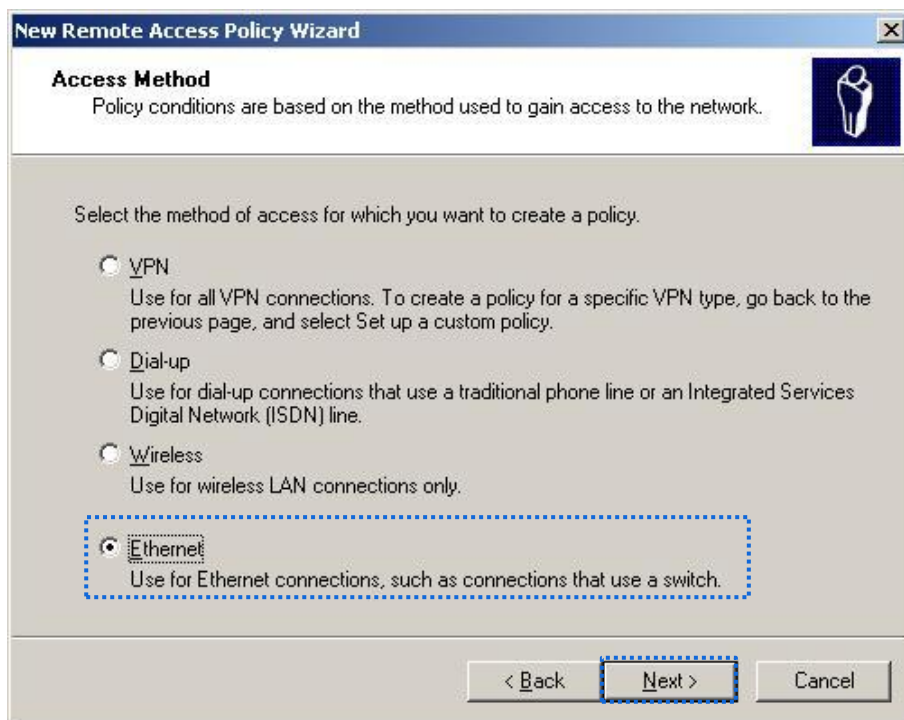
In the **New Remote Access Policy Wizard** dialog box that appears, click **Next**.



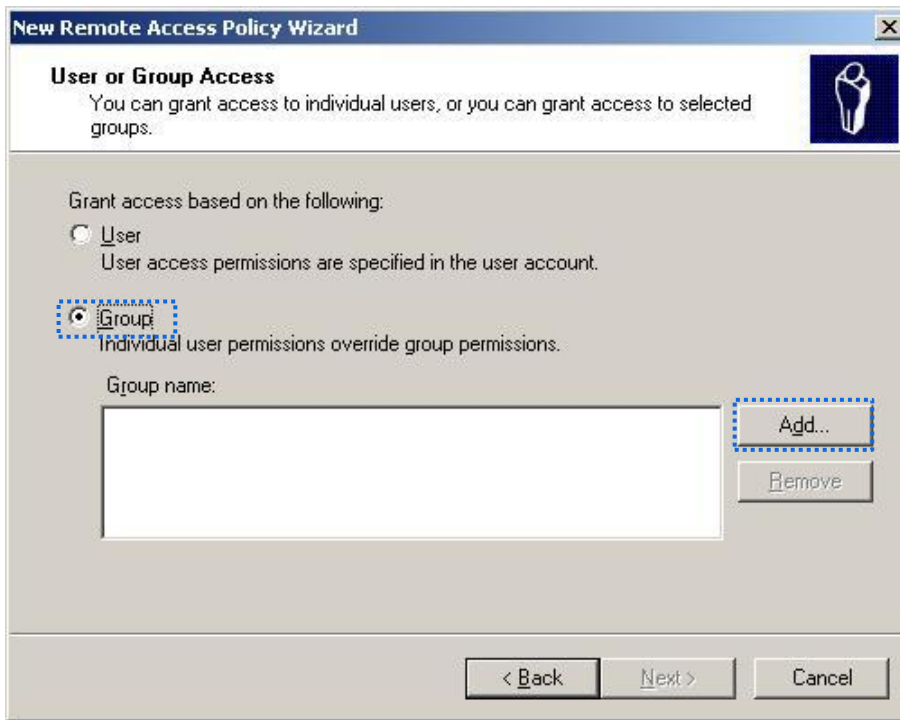
Enter a policy name and click **Next**.



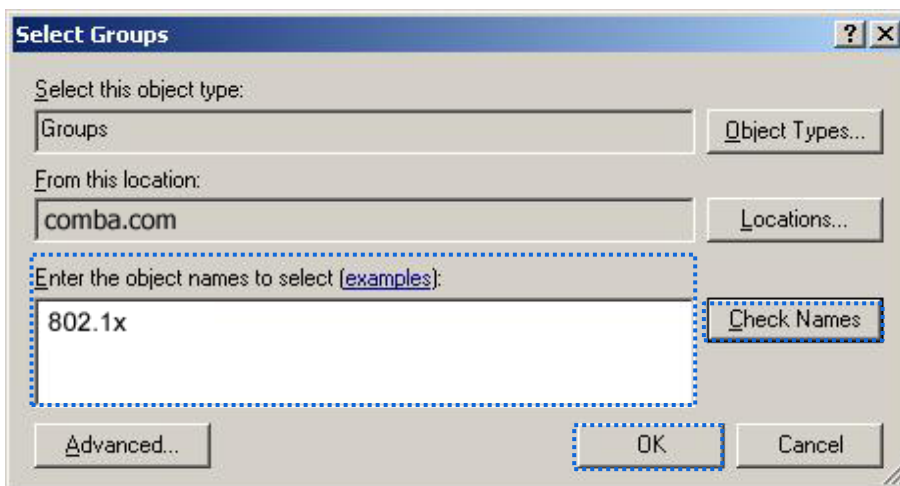
Select **Ethernet** and click **Next**.



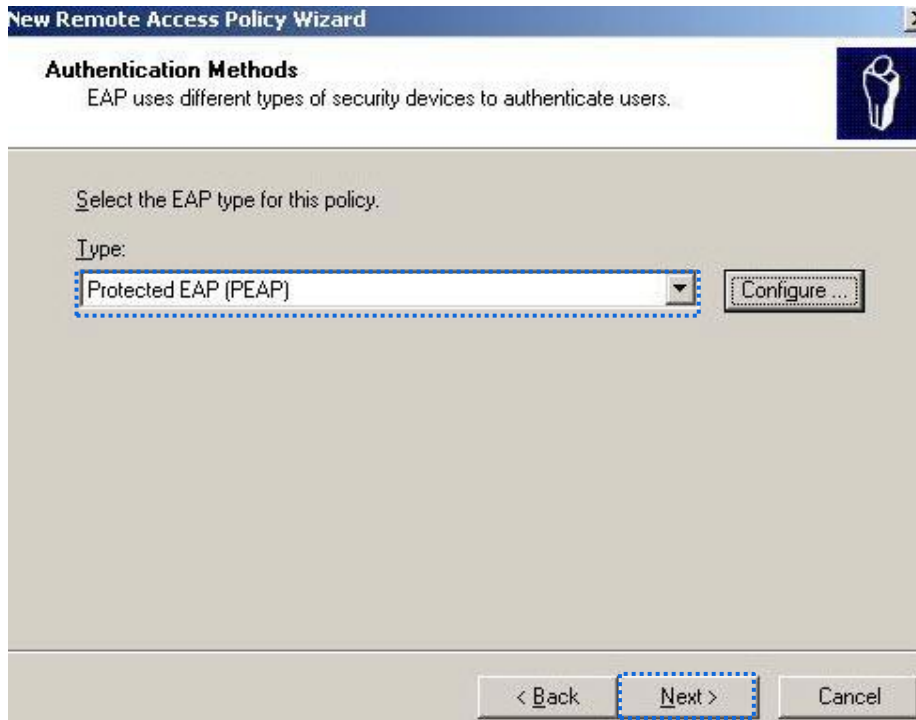
Select **Group** and click **Add**.



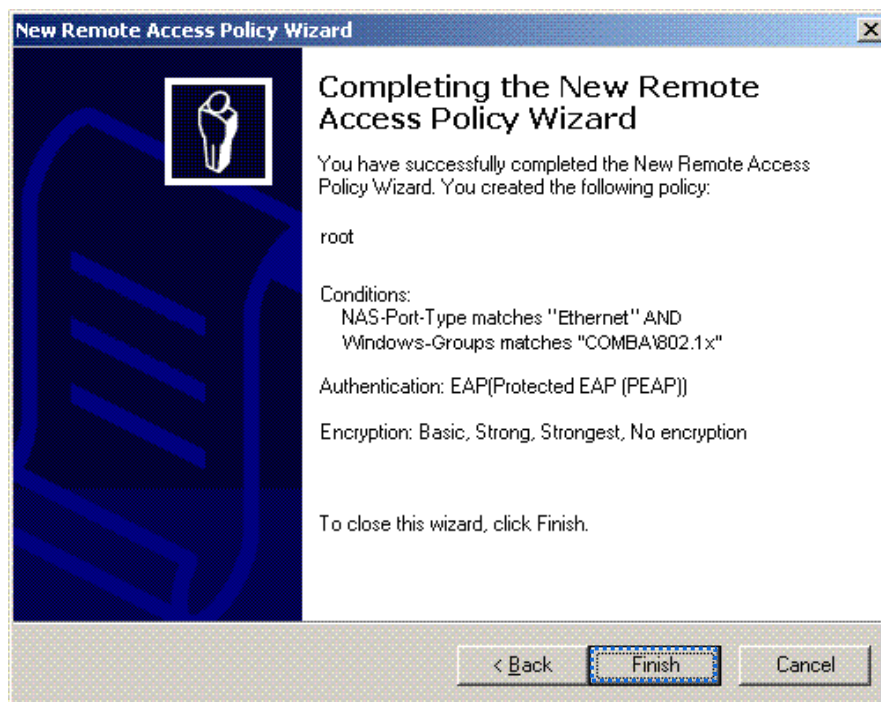
Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



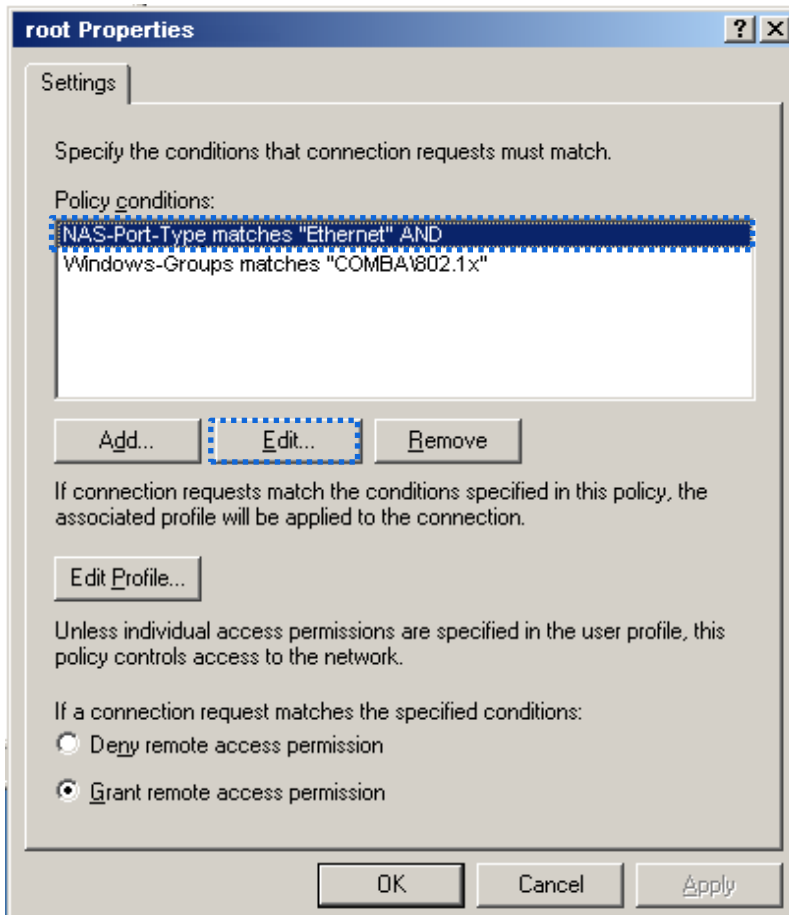
Select **Protected EAP (PEAP)** and click **Next**.



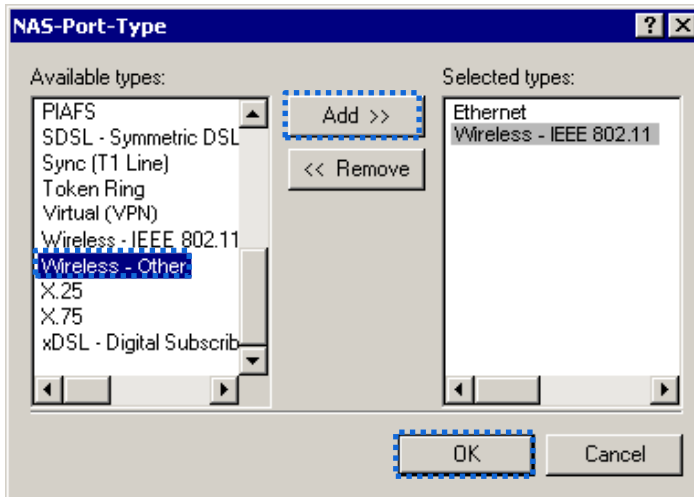
Click **Finish**. The remote access policy is created.



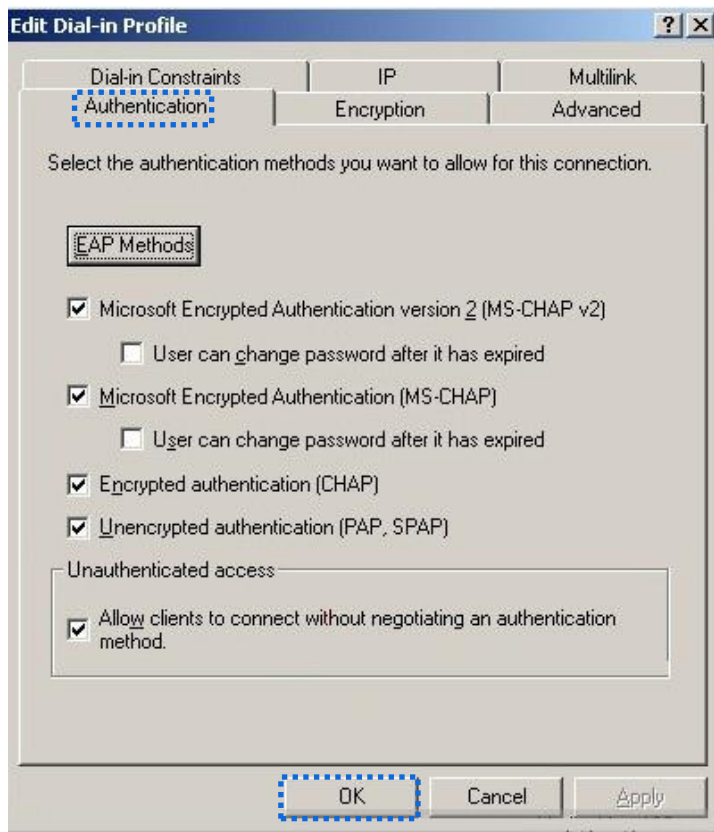
Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



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**.

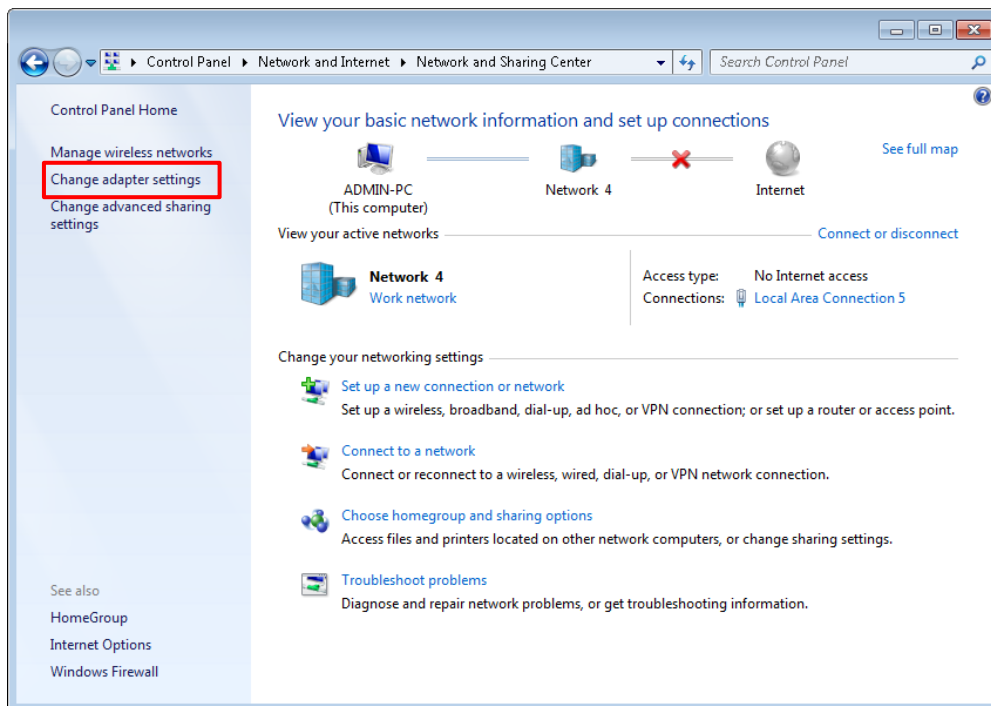
---End

Configure your wireless device.

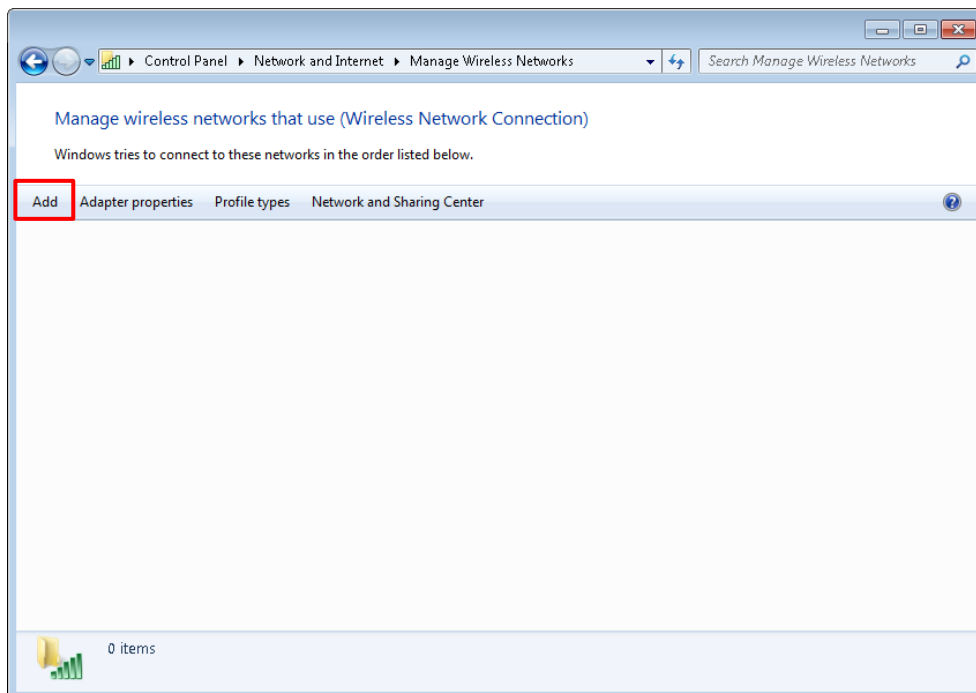


Windows 7 is taken as an example to describe the procedure.

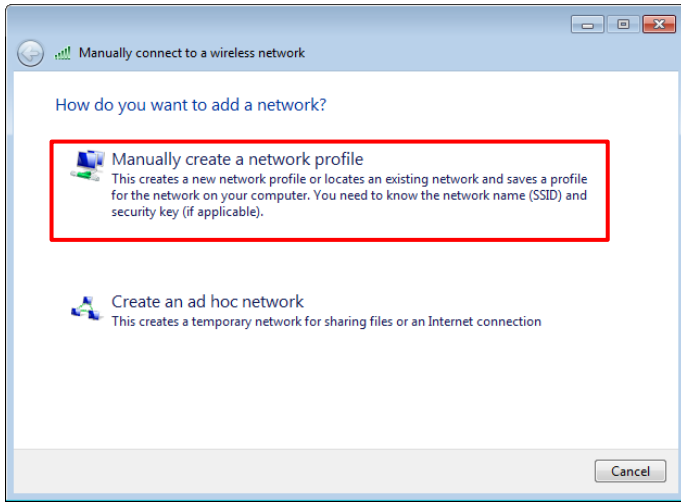
Choose **Start > Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



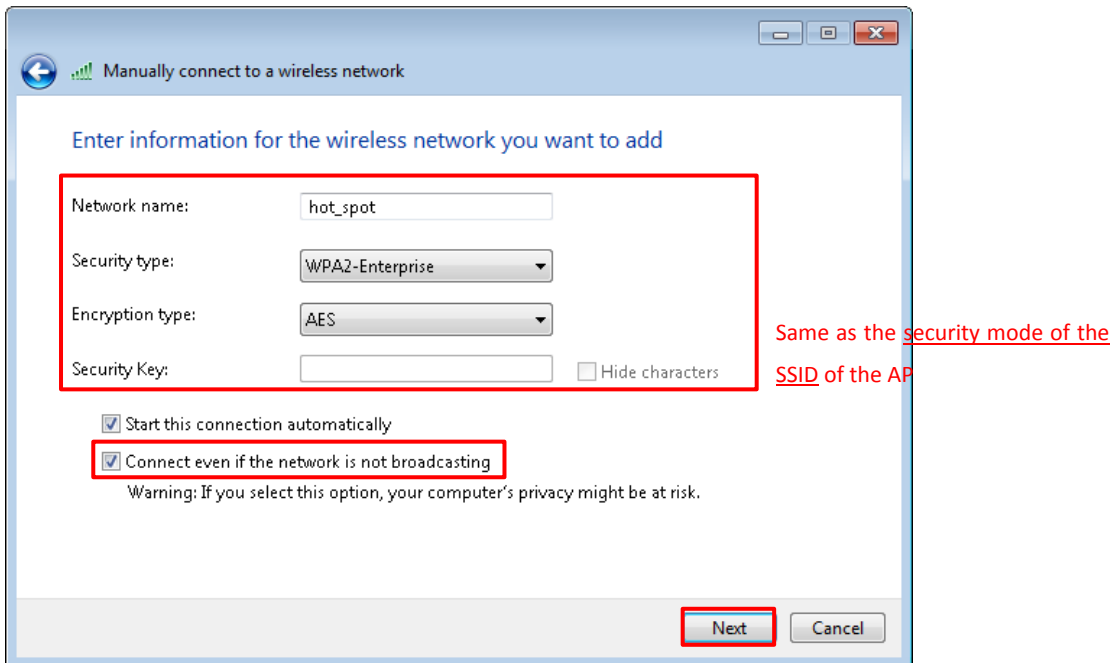
Click **Add**.



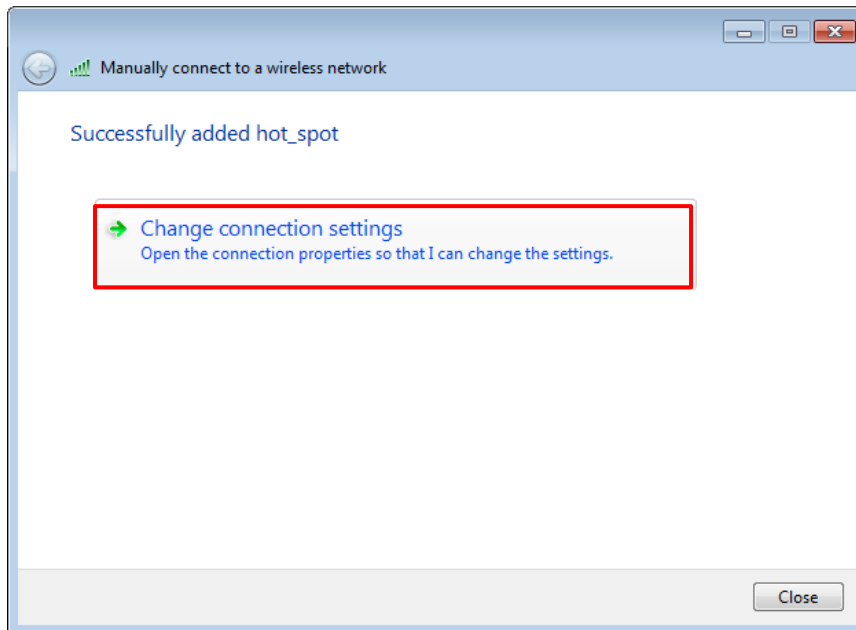
Click **Manually create a network profile**.



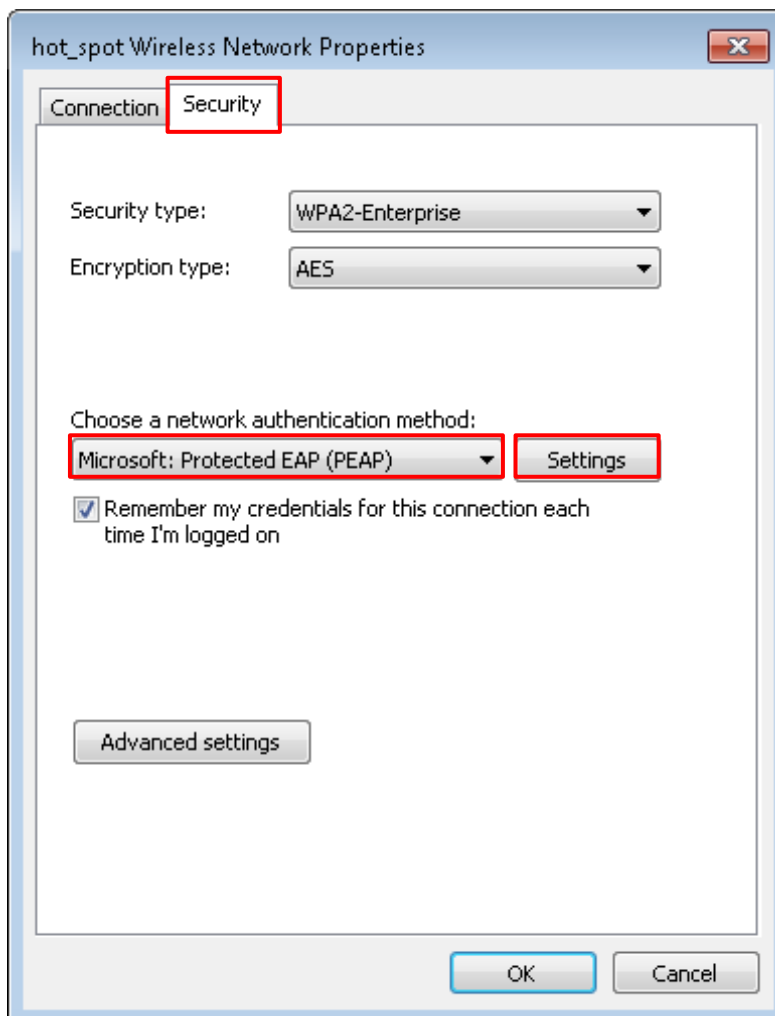
Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.



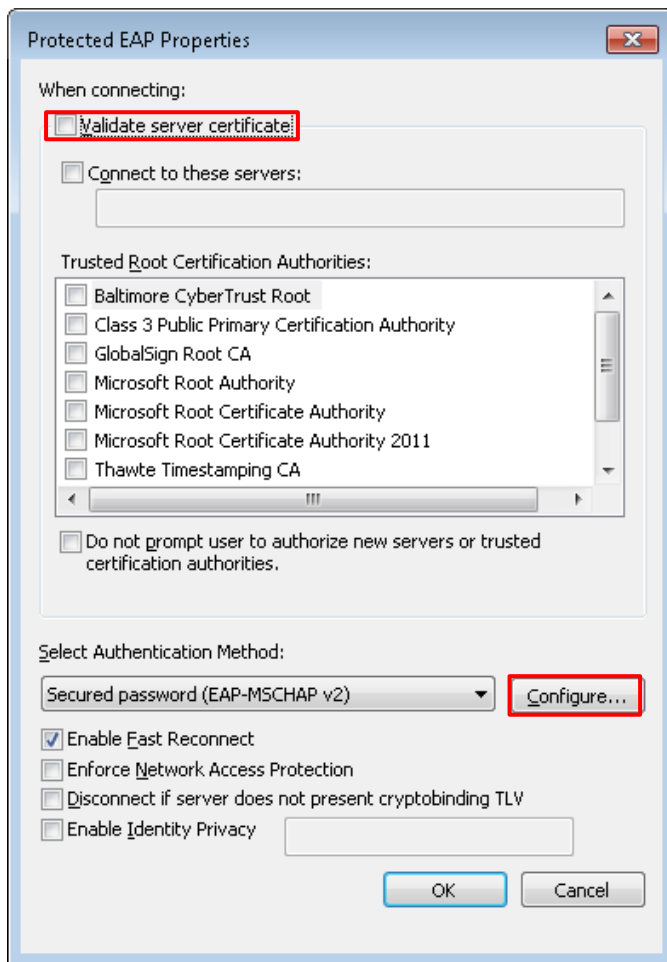
Click **Change connection settings**.



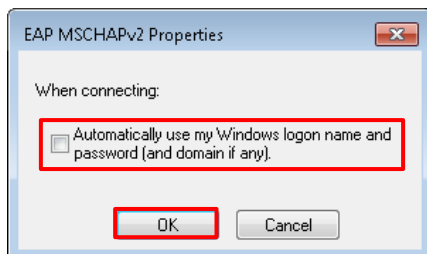
Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



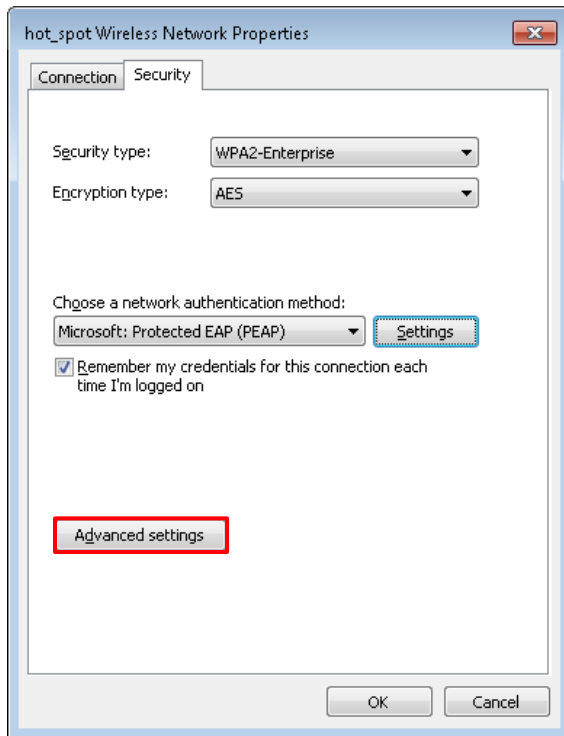
Deselect **Validate server certificate** and click **Configure**.



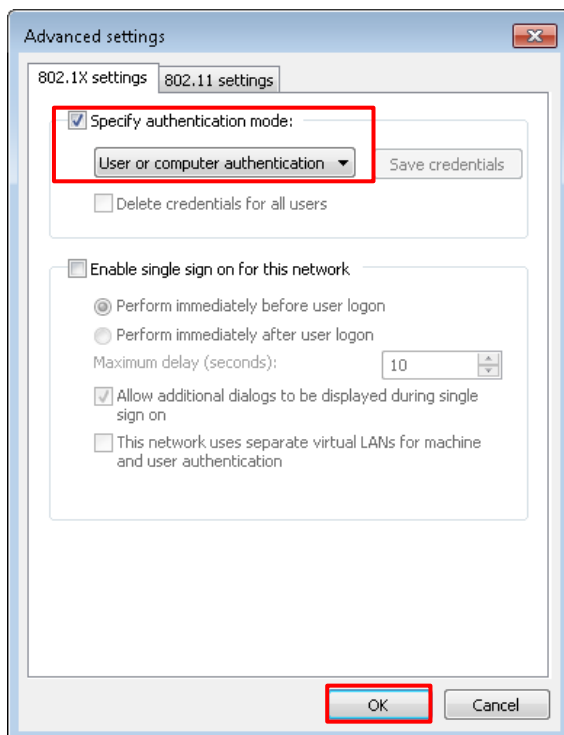
Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



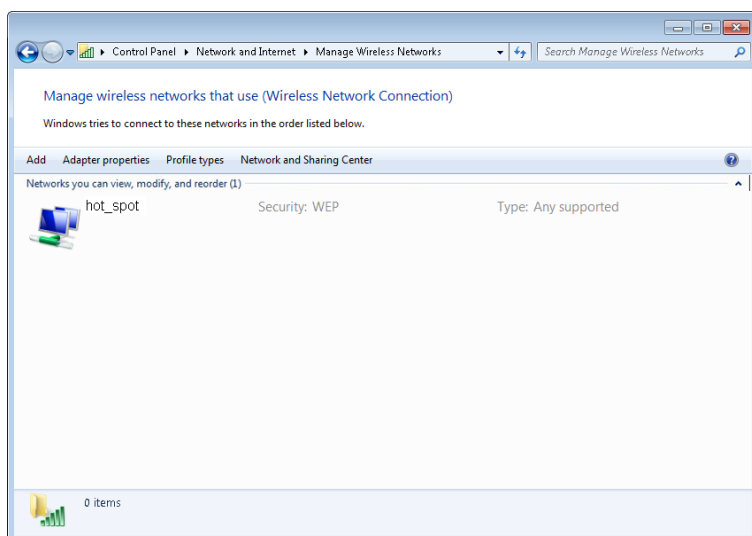
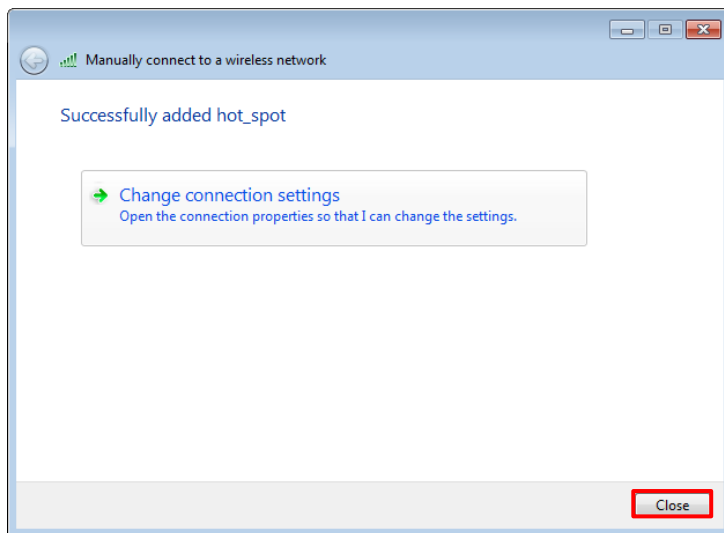
Click **Advanced settings**.



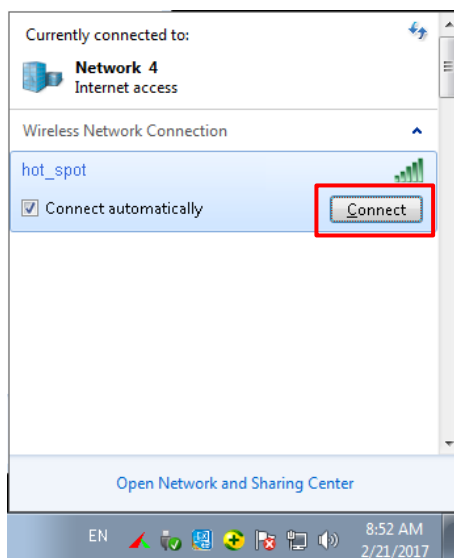
Select **User or computer authentication** and click **OK**.



Click **Close**.

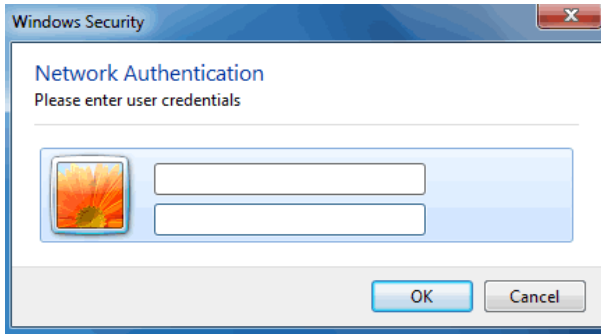


Click the network icon in the lower-right corner of the desktop and choose the wireless network of the AP, such as **hot_spot** in this example.



In the Windows Security dialog box that appears, enter the [user name and password](#) set on the RADIUS

server and click **OK**.



7.1.3.1.2 Verification

Wireless devices can connect to the wireless network hot_spot.

7.2 Radio Status

7.2.1 Overview

The **Radio** module is used to set Radio parameters of the AP. The following briefly describes the SSID isolation function.

SSID isolation

This function isolates the wireless clients connected to different wireless networks of the AP. For example, if user 1 connects to the wireless network corresponding to SSID1, whereas user 2 connects to the wireless network corresponding to SSID2, the two users cannot communicate with each other after SSID isolation is implemented.



7.2.2 Changing the Radio Settings

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

Radio

* Enable Wireless	<input checked="" type="checkbox"/>		<input type="button" value="Save"/>
Country/Region		<input type="text" value="China"/>	
Network Mode		<input type="text" value="11b/g/n mixed"/>	<input type="button" value="Restore"/>
* Channel		<input type="text" value="Auto"/>	<input type="button" value="Help"/>
Channel Bandwidth		<input type="radio"/> 20 <input type="radio"/> 40 <input checked="" type="radio"/> 20/40	
Extension Channel		<input type="text"/>	
* Channel Lockout		<input checked="" type="checkbox"/>	
SSID isolation		<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
APSD		<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Aging Time		<input type="text" value="5 minutes"/>	

---End

Parameter description

Parameter	Description
Enable Wireless	It specifies whether to enable the wireless function of the AP.
Country/Region	It specifies the country or region where the AP is used. This parameter helps comply with channel regulations of the country or region. The default value is China .
Network Mode	<p>It specifies the wireless network mode of the AP. Available options include 11b/g/n mixed, 11b, 11g, 11b/g/n mixed. This parameter can be set if Channel Lockout is not selected.</p> <ul style="list-style-type: none"> ■ 11b: The AP works in 802.11b mode and only wireless devices compliant with 802.11b can connect to the wireless networks of the AP. ■ 11g: The AP works in 802.11g mode and only wireless devices compliant with 802.11g can connect to the wireless networks of the AP. ■ 11b/g: The AP works in 802.11b/g mode and only wireless devices compliant with 802.11b or 802.11g can connect to the wireless networks of the AP. ■ 11b/g/n: The AP works in 802.11b/g/n mode. Wireless devices compliant with 802.11b or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n can connect to the wireless networks of the AP.
Channel	<p>It specifies the operating channel of the AP. This parameter can be set if Channel Lockout is not selected.</p> <p>Auto: It indicates that the AP automatically adjusts its operating channel according to the ambient environment.</p>
Channel Bandwidth	<p>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 Channel Lockout is not selected.</p> <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. ■ 20/40: It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment.
Expansion Channel	It specifies the wireless expansion channel of the AP. This parameter can be set if the channel bandwidth of the AP is set to 40 or 20/40 and Channel Lockout is not selected.

Parameter	Description
Channel Lockout	It is used to lock the channel settings of the AP. If this parameter is selected, channel settings including Country/Region , Network Mode , Channel , Channel Bandwidth , and Expansion Channel cannot be changed.
SSID isolation	It specifies whether to isolate the wireless clients connected to the AP with different SSIDs. <ul style="list-style-type: none">■ Disable: It indicates that the wireless clients connected to the AP with different SSIDs can communicate with each other.■ Enable: It indicates that the wireless clients connected to the AP with different SSID cannot communicate with each other. This improves wireless network security.
APSD	It specifies whether to enable the Automatic Power Save Delivery (APSD) function. It helps reduce power consumption of the AP. By default, it is disabled.
Aging Time	It is used to set the aging time of clients. After a wireless client connects to the AP, the AP disconnects from the wireless client if no data is exchanged between them within the interval.

7.3 Channel Scan

7.3.1 Overview

This function enables you to learn about the wireless signals near the AP, including information about SSID, MAC address, channel, and signal strength. The information helps you choose a relatively idle channel for the AP to improve wireless transmission efficiency.

7.3.2 Scanning Channels

1. Choose **Wireless > Channel Scan**.
2. Click **Scan**.



---End

The following picture displays the scanning results.

The screenshot shows the 'Signal Scan' interface displaying scanning results. At the top, there is a red header with the text 'Signal Scan'. Below the header, there is a section titled 'Channel Scan' with a button labeled 'Disable Scan' and a 'Help' button on the right. The main content is a table with 8 columns: ID, SSID, MAC Address, Network Mode, Channel, Bandwidth, Security, and Signal Strength. The table contains 8 rows of data.

ID	SSID	MAC Address	Network Mode	Channel	Bandwidth	Security	Signal Strength
1	PSST-CESHI-TLJ-A9TDC22	50:2b:73:10:42:10	bgn	11	40	wpa&wpa2/aes	-30dBm
2	TP-LINK_F731	14:cc:20:e5:f7:31	bgn	1	20	wpa&wpa2/aes&tkip	-30dBm
3	zhangsan	c8:3a:35:1e:ac:60	bgn	11	20	wpa&wpa2/aes	-30dBm
4	Tenda_C0004E	50:2b:73:c0:00:4e	bgn	6	40	wpa2/aes	-30dBm
5	Tenda_F99999	c8:3a:35:f9:99:99	bgn	11	20	wpa&wpa2/aes	-30dBm
6	AC15_liu	c8:3a:35:1e:ae:85	bgn	11	20	wpa&wpa2/aes	-30dBm
7	Tenda_test	c8:90:4c:a8:88:a2	bgn	7	20	wpa&wpa2/aes	-34dBm
8	IP-COM_AP_0	00:b0:c6:4c:0f:01	bgn	7	20	none	-34dBm

7.4 WMM Settings

7.4.1 Overview

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

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

WMM involves the following terms:

- Enhanced Distributed Channel Access (EDCA): It is a channel competition mechanism to ensure that packets with higher priorities are assigned more bandwidth and transmitted earlier.
- Access Category (AC): 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.

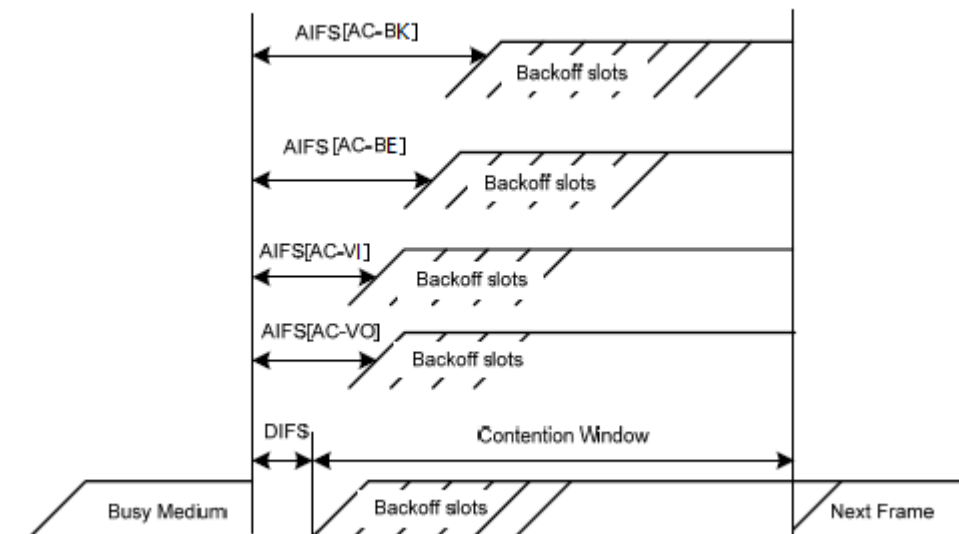
■ EDCA Parameters

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

WMM assigns different channel competition parameters to each AC.



■ 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.

7.4.2 Changing the WMM Settings

By default, the WMM function of the AP is enabled and the **Optimized For Capacity** mode is adopted. Procedure for changing the WMM settings:

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

WMM Setup

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	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="6"/>	<input type="text" value="0"/>
AC_BK	<input type="text" value="1"/>	<input type="text" value="5"/>	<input type="text" value="8"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1"/>	<input type="text" value="3008"/>
AC_VO	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="1"/>	<input type="text" value="1504"/>

EDCA STA Parameters

	CWmin	CWmax	AIFSN	TXOP Limit(usec)
AC_BE	<input type="text" value="2"/>	<input type="text" value="5"/>	<input type="text" value="8"/>	<input type="text" value="0"/>
AC_BK	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="7"/>	<input type="text" value="0"/>
AC_VI	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="2"/>	<input type="text" value="3008"/>
AC_VO	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="2"/>	<input type="text" value="1504"/>

---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 clients are connected to the AP, you are recommended to select this mode to increase client throughput. ■ Optimized For Capacity: If more than 10 clients are connected to the AP, you are recommended to select this mode to ensure client connectivity. ■ Custom: This mode enables you to set the WMM EDCA parameters for manual optimization.
No ACK	<ul style="list-style-type: none"> ■ If the check box is selected, the No ACK policy is adopted. ■ If the check box is deselected, the Normal ACK policy is adopted.
EDCA Parameters	For details, refer to section 7.4.1 "Overview."

7.5 Advanced

7.5.1 Overview

This module is used to set the RF performance optimization parameters of the AP.

7.5.2 Changing the Advanced Settings



It is recommended that you change the settings only under the instruction of professional personnel, so as to prevent decreasing the wireless performance of the AP.

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

Advanced

Beacon Interval	<input type="text" value="100"/> (Range: 20 - 999; Default: 100)	<input type="button" value="Save"/>
Fragment Threshold	<input type="text" value="2346"/> (Range: 256 - 2346; Default: 2346)	<input type="button" value="Restore"/>
RTS Threshold	<input type="text" value="2347"/> (Range: 1 - 2347; Default: 2347)	<input type="button" value="Help"/>
DTIM Interval	<input type="text" value="1"/> (Range: 1 - 255; Default: 1)	
Receive Signal strength	<input type="text" value="-90"/> (dBm, Range: -90 - -60; Default: -90)	
TX Power	<input type="text" value="18"/> (dBm, Range: 8 - 18; Default: 18)	
Power Lockout	<input checked="" type="checkbox"/>	
Preamble	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble	

---End

Parameter description

Parameter	Description
Beacon Interval	<p>It specifies the interval for transmitting the Beacon frame. The value range is 20 to 999. The unit is 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 clients to connect to the AP more quickly, while a larger interval ensures higher data transmission efficiency.</p>
Fragment Threshold	<p>It specifies the threshold of a fragment. The value range is 256 to 2346. The default value is 2346. The unit is 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>

Parameter	Description
	<p>In case of a high error rate, you can reduce the threshold to enable the AP to resend only the fragments that have not been sent successfully, so as to increase the frame throughput.</p> <p>In an environment without interference, you can increase the threshold to reduce the number of acknowledgement times, so as to increase the frame throughput.</p>
RTS Threshold	<p>It specifies the frame length threshold for triggering the RTS/CTS mechanism.</p> <p>If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The value range is 1 to 2347. The unit is 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 wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold for reducing conflicts.</p> <p>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. The unit is 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>
Receive Signal Strength	<p>It specifies the minimum strength of received signals acceptable to the AP. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to the AP.</p> <p>If there are multiple APs, an appropriate value of this parameter ensures that wireless clients connect to the APs with strong signals.</p>
Power	<p>It specifies the transmit power of the AP. This parameter can be set if Lock Power is not selected.</p> <p>A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the wireless network performance and security.</p>
Power Lockout	<p>It specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.</p>
Preamble	<p>It specifies whether to use long preamble or short preamble. A preamble is a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data.</p> <p>By default, the Long Preamble option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the Short Preamble option.</p>

7.6 Access Control

7.6.1 Overview

It specifies, based on MAC address filter rules, the wireless devices that can or cannot access the wireless networks of the AP. Devices that have been controlled cannot connect to the corresponding wireless network.

The AP supports the following MAC address filter rules:

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

7.6.2 Configuring Access Control

1. Choose **Wireless > Access Control**.
2. From the **SSID** drop-down list box, select the SSID of the wireless network on which access control must be implemented.
3. Select an access control mode from the **MAC Filter Mode** drop-down list box.
4. If you select **Allow** or **Disallow**, enter the MAC addresses to control in the access control list and click **Add**.

If a wireless device to be controlled has been connected to the AP, you can click **Add** corresponding to the device in the wireless client list to directly add it to the access control list.

5. Click **Save**.

Control

Specify a list of devices to allow or disallow a connection to your wireless network via the devices' MAC addresses. This can be set separately on each SSID.

SSID: IP-COM_AP_0

MAC Filter Mode: Allow

Save Restore Help

ID	MAC Address	IP	Connection Duration	Add to List
1	A0:8D:16:42:43:21	192.168.0.135	00:00:02	Add

MAC Address: [] : [] : [] : [] : [] : []

Action: Add

ID	MAC Address	Action
1	A0:8D:16:42:43:21	<input checked="" type="checkbox"/> Enable Delete

Parameter description

Parameter	Description
SSID	It specifies the SSID that requires wireless client access control.
MAC Filter Mode	It specifies the mode for filtering MAC addresses. <ul style="list-style-type: none">■ Disable: It indicates that access control is disabled.■ Allow: It indicates that only the wireless clients on the access control list can connect to the AP with the selected SSID.■ Disallow: It indicates that only the wireless clients on the access control list cannot connect to the AP with the selected SSID.

7.6.3 Example of Configuring Access Control

Networking requirement

A wireless network whose SSID is Home has been set up in a large apartment. Only family members are allowed to connect to the wireless network.

The Access Control function of the AP is recommended. The family members have three wireless devices whose MAC addresses are C8:3A:35:00:00:01, C8:3A:35:00:00:02, and C8:3A:35:00:00:03.

Configuration procedure

1. Choose **Wireless > Access Control**.
 2. Select **Home** from the **SSID** drop-down list box.
 3. Select **Allow** from the **MAC Filter Mode** drop-down list box.
 4. Enter **C8:3A:35:00:00:01** in the **MAC Address** text box 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 configuration.

Control

Specify a list of devices to allow or disallow a connection to your wireless network via the devices' MAC addresses. This can be set separately on each SSID.

SSID: HOME

MAC Filter Mode: Allow

Save Restore Help

ID	MAC Address	IP	Connection Duration	Add to List
No clients connected!				

MAC Address: []:[]:[]:[]:[]:[]

Action: Add

ID	MAC Address	Connection Duration	Action
1	C8:3A:35:00:00:01	<input checked="" type="checkbox"/> Enable	Delete
2	C8:3A:35:00:00:02	<input checked="" type="checkbox"/> Enable	Delete
3	C8:3A:35:00:00:03	<input checked="" type="checkbox"/> Enable	Delete

Verification

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

7.7 QVLAN

7.7.1 Overview

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

7.7.2 Configuring the QVLAN Function

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

QVLAN Setup

*** Enable**

PVID

Manage VLAN

Trunk Port LAN0 LAN1

Wired LAN Port	VLAN ID (1~4094)
LAN0	<input type="text" value="1"/>
LAN1	<input type="text" value="1"/>


2.4G SSID	VLAN ID (1~4094)
IP-COM_AP_0	<input type="text" value="1000"/> *
HOME	<input type="text" value="1000"/>

Save **Restore** **Help**

---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.
Trunk Port	It specifies the LAN port used as a trunk port of the AP. The default value is LAN0 . Traffic of all VLANs can pass through a trunk port.

 **TIP**

Parameter	Description
	<i>If the QVLAN function is enabled, set at least one LAN port as a trunk port. LAN0 indicates the LAN port at the rear of the AP, whereas LAN1 indicates the LAN port at the front of the AP.</i>
LAN Port	It specifies the LAN ports of the AP, including LAN0 and LAN1.
VLAN ID	It specifies the VLAN ID corresponding to a LAN port used as an access port.
2.4G SSID	It specifies the currently enabled SSIDs of the AP.
VLAN ID	It specifies VLAN IDs corresponding to SSIDs. The default value is 1000 . The value range is 1 to 4094. After the QVLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID and VLAN ID of an access port are the same.

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	If the VID and PVID of a port are the same, transmit data after removing tags from the data. If the VID and PVID of a port are different, transmit data without removing tags from the data.

7.7.3 Example of Configuring QVLAN Settings

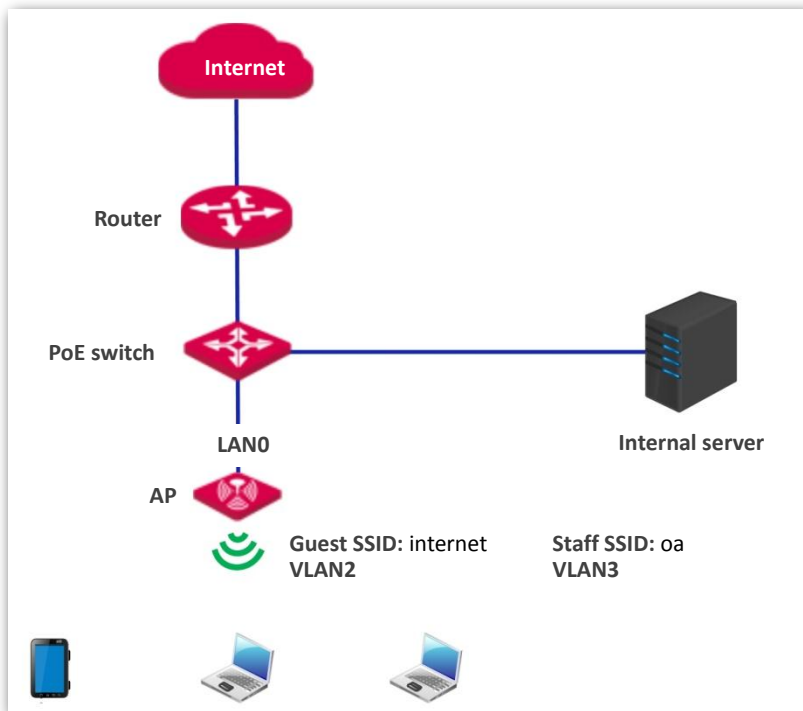
Networking requirement

A hotel has the following wireless network coverage requirements:

- Guests are connected to VLAN 2 and can access only the internet.
- Employees are connected to VLAN 3 and can access only the LAN.

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

Network topology



Configuration procedure

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**.

QVLAN Setup

* Enable

PVID

Manage VLAN

Trunk Port LAN0 LAN1

Save

Restore

Help

Wired LAN Port	VLAN ID (1~4094)
LAN0	<input type="text" value="1"/>
LAN1	<input type="text" value="1"/>

2.4G SSID	VLAN ID (1~4094)
internet	<input type="text" value="2"/> *
oa	<input type="text" value="3"/> *

---End

Wait for the automatic reboot of the AP.

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
LAN server	3	Access	3
Router	2	Access	2

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

Verification

Wireless clients connected to the **internet** wireless network can access only the internet, whereas the wireless clients connected to the **oa** wireless network can access only the LAN.。

8 SNMP

8.1 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 receive network event alarms.

SNMP allows automatic management of devices from various vendors regardless of physical differences among the devices.

8.1.1 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. The SNMP manager most widely used in network environments is Network Management System (NMS). 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. The 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. It defines a series of attributes of managed objects, including names, access permissions, and data types of objects. Each SNMP agent has its 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.

8.1.2 Basic SNMP Operations

The AP allows 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.

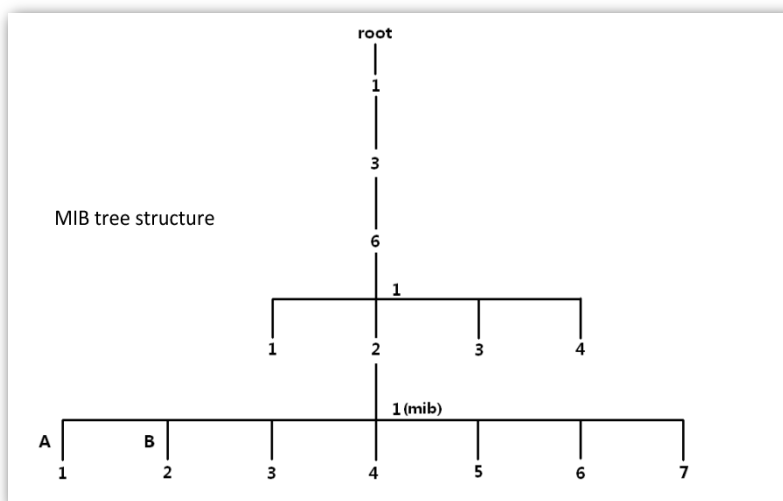
8.1.3 SNMP Protocol Version

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.

8.1.4 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.




8.2 Configuring the SNMP Function

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

SNMP
Here you can configure SNMP settings. SNMP v1 and v2c are supported.
SNMP Agent Disable Enable
Administrator Name
Device Name
Location
Read Community
Read/Write Community

---End

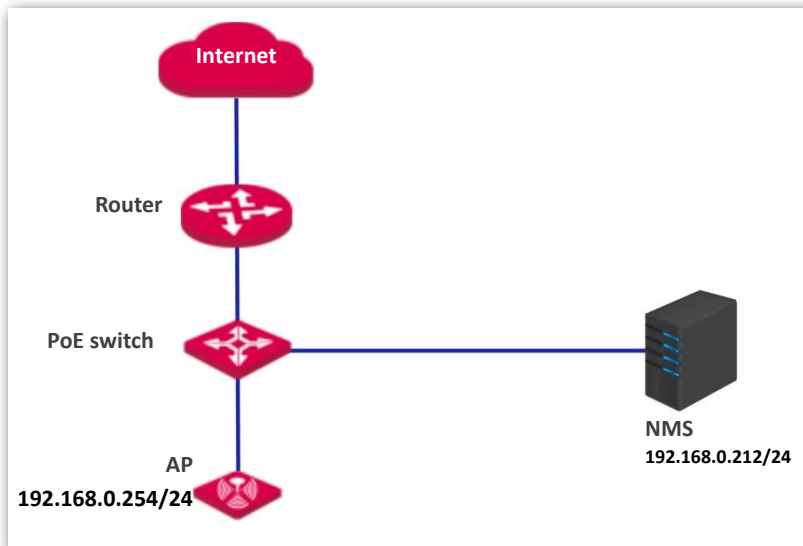
Parameter description

Parameter	Description
SNMP Agent	<p>It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled.</p> <p>An SNMP manager and the SNMP agent can communicate with each other only if their SNMP versions are the same. Currently, the SNMP agent function of the AP supports SNMP V1 and SNMP V2C.</p>
Administrator	<p>It specifies the name of the administrator of the AP. The default name is Administrator. You can change the location as required.</p>
Device Name	<p>It specifies the device name of the AP. The default device name is the model of the AP. For example, the default name of W30AP V4.0 is W30APV4.0.</p> <p> TIP</p> <p>It is recommended that you change the AP name so that you can easily identify the AP when managing the AP using SNMP.</p>
Location	<p>It specifies the location where the AP is used. You can change the location as required.</p>
Read Community	<p>It specifies the read password shared between SNMP managers and this SNMP agent. The default password is public.</p> <p>The SNMP agent function of the AP allows an SNMP manager to use the password to read variables in the MIB of the AP.</p>
Read/Write Community	<p>It specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is private.</p> <p>The SNMP agent function of the AP allows an SNMP manager to use the password to read/write variables in the MIB of the AP.</p>

8.3 Example of Configuring the SNMP Function

Networking requirement

- The AP connects to an NMS over an LAN. 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 use SNMP V1 or SNMP V2C to monitor and manage the AP.



Configuration procedure

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**.

SNMP

Here you can configure SNMP settings. SNMP v1 and v2c are supported.

SNMP Agent	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Save
Administrator Name	<input type="text" value="Tom"/>	Restore
Device Name	<input type="text" value="W30APV4.0"/>	Help
Location	<input type="text" value="ShenZhen"/>	
Read Community	<input type="text" value="Tom"/>	
Read/Write Community	<input type="text" value="Tom123"/>	

---End

Configure the NMS.

On an NMS that uses SNMP V1 or SNMP V2C, set the read community to **Tom** and read/write community to **Tom 123**. For details about how to configure the NMS, refer to the configuration guide for the NMS.

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.

9 Deployment

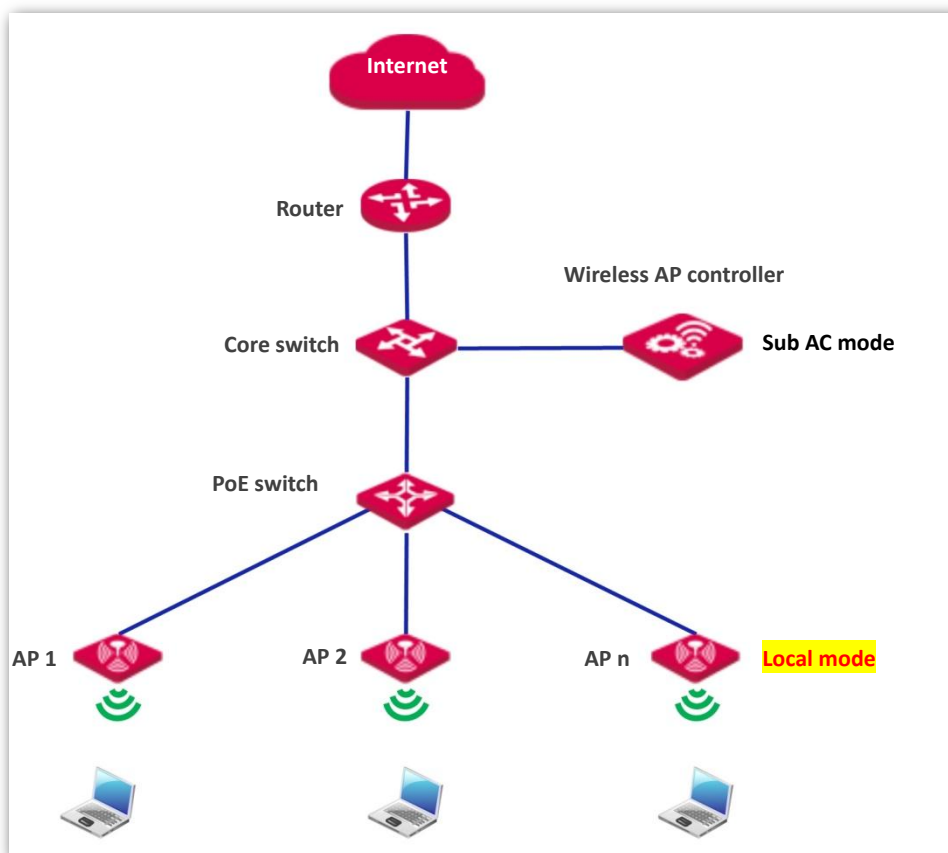
9.1 Overview

If a large number of APs are deployed, you are recommended to adopt an IP-COM AP controller (AC1000/2000/3000. AC2000 is used as an example) to manage the APs in a centralized manner.

In this case, **Local** and **Cloud** deployment modes are supported.

- Local Deployment

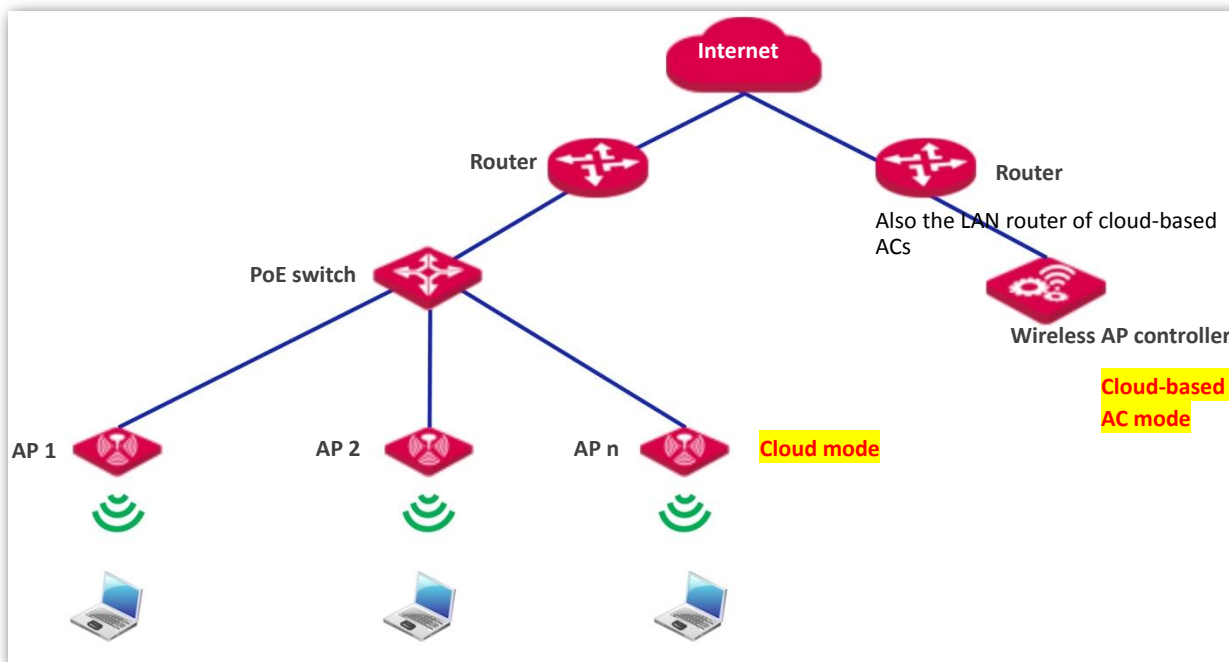
If you need to deploy many APs in a small area, you are recommended to select the local deployment mode, which uses a local AC (in Sub AC mode) to manage the APs in a centralized manner. The following figure shows the topology for the local deployment mode.



- 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.



9.2 Configuring the Deployment Mode

By default, the deployment mode of the AP is Local.

9.2.1 Configuring Local Deployment Mode

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

Deployment	
Deployment	<input checked="" type="radio"/> Local <input type="radio"/> Cloud
Device Name	<input type="text" value="W30APV4.0"/>
Cloud AC Address	<input type="text"/>
(The WAN IP address of the router that the Root AC connects to)	
Cloud AC Manage Port	<input type="text"/> (Valid Range: 1024~65535)
Cloud AC Upgrade Port	<input type="text"/> (Valid Range: 1024~65535)

Buttons: Save, Restore, Help

---End

9.2.2 Configuring Cloud Deployment Mode

1. Choose **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**.

Deployment

Deployment Local Cloud Save

Device Name Restore

Cloud AC Address Help

(The WAN IP address of the router that the Root AC connects to)

Cloud AC Manage Port (Valid Range: 1024~65535)

Cloud AC Upgrade Port (Valid Range: 1024~65535)

---End

Parameter description

Parameter	Description
Deployment	<p>It specifies the deployment mode of the AP. The default option is Local.</p> <ul style="list-style-type: none">■ Local: It indicates that the AP can be managed only through the AC connected to the local network (AC in the same local area network).■ Cloud: In this mode, the AP can be managed only by a cloud AC. To use the cloud deployment mode, set the following parameters as well.
Device Name	<p>It specifies the device name of the AP. The default device name is the model of the AP.</p> <p>You are recommended to change the device name so that you can quickly locate the AP when managing the AP remotely.</p>
Cloud AC Address	<p>It specifies the WAN IP address of the router to which the cloud AC connects, or the domain name to which the WAN IP address is bound.</p>
Cloud AC Manage Port	<p>It specifies the port of the router to which the cloud AC connects for managing APs.</p>
Cloud AC Upgrade Port	<p>It specifies the port of the router to which the cloud AC connects for managing APs.</p>

10 Tools

10.1 Firmware Upgrade

This function upgrades the firmware of the AP for more functions and higher stability.



To prevent damaging the AP, verify that the new firmware version is applicable to the AP before upgrading the firmware and keep the power supply of the AP connected during an upgrade.

Procedure:

1. Download the package of a later firmware version for the AP from <http://www.ip-com.com.cn> to your local computer, and decompress the package.
2. Log in to the web UI of the AP and choose **Tools > Firmware Upgrade**.
3. Click **Choose File** and select the file for upgrading the firmware.
4. Click **Upgrade**.

Firmware Upgrade

Use this section to update device's firmware for better functionalities or new features.

Select a Firmware File: No file chosen

Current Firmware Version: V1.0.0.2(477); Release Date: 2017-02-18

Note: DO NOT disconnect the device from power and network connections while upgrade is in process, otherwise it may be permanently damaged. When upgrade is complete, the device restarts automatically. Upgrade may take about 90 seconds. Please wait.

---End

Wait until the progress bar is complete. Log in to the web UI of the AP again. Choose **Status > System Status** and check whether the upgrade is successful based on **Firmware Version**.



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.

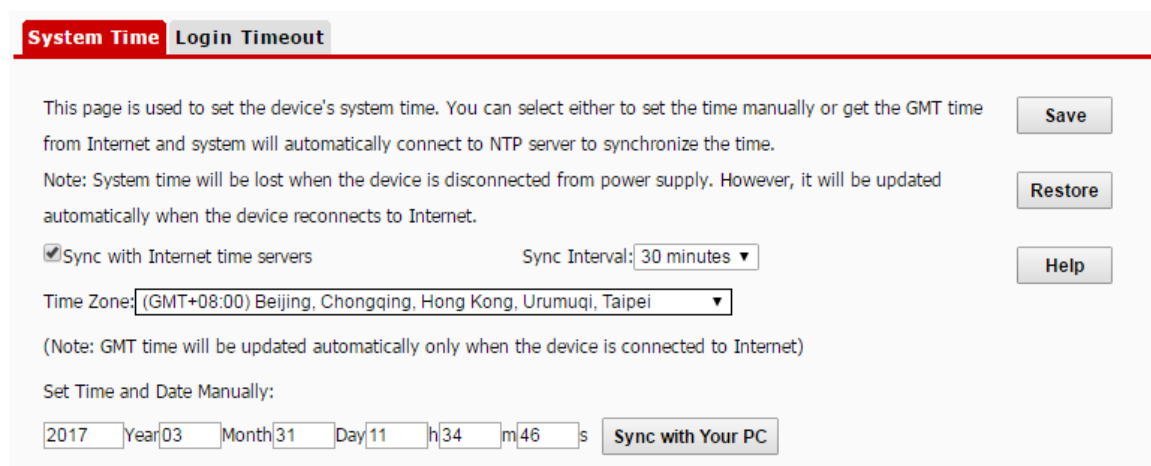
10.2 Time & Date

This module enables you to set the [system time](#) and [login timeout](#) interval of the AP.

10.2.1 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, choose **Tools > Time and Date**.



The screenshot shows the 'System Time' configuration page. At the top, there are two tabs: 'System Time' (selected) and 'Login Timeout'. Below the tabs, there is a red horizontal line. The main content area contains the following elements:

- A paragraph: "This page is used to set the device's system time. You can select either to set the time manually or get the GMT time from Internet and system will automatically connect to NTP server to synchronize the time." To the right of this paragraph is a 'Save' button.
- A note: "Note: System time will be lost when the device is disconnected from power supply. However, it will be updated automatically when the device reconnects to Internet." To the right of this note is a 'Restore' button.
- A checked checkbox labeled 'Sync with Internet time servers' and a 'Sync Interval' dropdown menu set to '30 minutes'. To the right of these is a 'Help' button.
- A 'Time Zone' dropdown menu set to '(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumuqi, Taipei'.
- A note: "(Note: GMT time will be updated automatically only when the device is connected to Internet)".
- A section titled 'Set Time and Date Manually:' with input fields for Year (2017), Month (03), Day (31), Hour (11), Minute (34), and Second (46). To the right of these fields is a 'Sync with Your PC' button.

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

Syn with Internet time servers

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

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

Procedure for configuring the AP to synchronize its system time with the internet:

1. Choose **Tools > Time and Date > System Time**.
2. Select the **Sync with Internet time servers** check box.
3. Set **Sync Interval** to the interval at which the AP synchronizes its system time with a time server of the internet. The default value **30 minutes** is recommended.
4. Set **Time Zone** to your time zone.
5. Click **Save**.

System Time Login Timeout

This page is used to set the device's system time. You can select either to set the time manually or get the GMT time from Internet and system will automatically connect to NTP server to synchronize the time.

Note: System time will be lost when the device is disconnected from power supply. However, it will be updated automatically when the device reconnects to Internet.

Sync with Internet time servers Sync Interval: 30 minutes ▼

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

(Note: GMT time will be updated automatically only when the device is connected to Internet)

Set Time and Date Manually:

2017 Year 03 Month 31 Day 11 h 34 m 46 s Sync with Your PC

Save

Restore

Help

---End

Set Time and Date Manually

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

Procedure:

1. Choose **Tools > Time and Date > System Time**.
2. Enter a correct date and time, or click **Sync with Your PC** to synchronize the system time of the AP with the system time (ensure that it is correct) of the computer being used to manage the AP.
3. Click **Save**.

System Time Login Timeout

This page is used to set the device's system time. You can select either to set the time manually or get the GMT time from Internet and system will automatically connect to NTP server to synchronize the time.

Note: System time will be lost when the device is disconnected from power supply. However, it will be updated automatically when the device reconnects to Internet.

Sync with Internet time servers Sync Interval: 30 minutes ▼

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

(Note: GMT time will be updated automatically only when the device is connected to Internet)

Set Time and Date Manually:

2017 Year 03 Month 31 Day 11 h 34 m 46 s Sync with Your PC

Save

Restore

Help

---End

10.2.2 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 for network security. The default login timeout interval is 5 minutes.

Procedure for setting the login timeout interval:

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

3. Click **Save**.

System Time **Login Timeout**

Login Timeout: (1~60 minutes)

Save

Restore

Help

---End

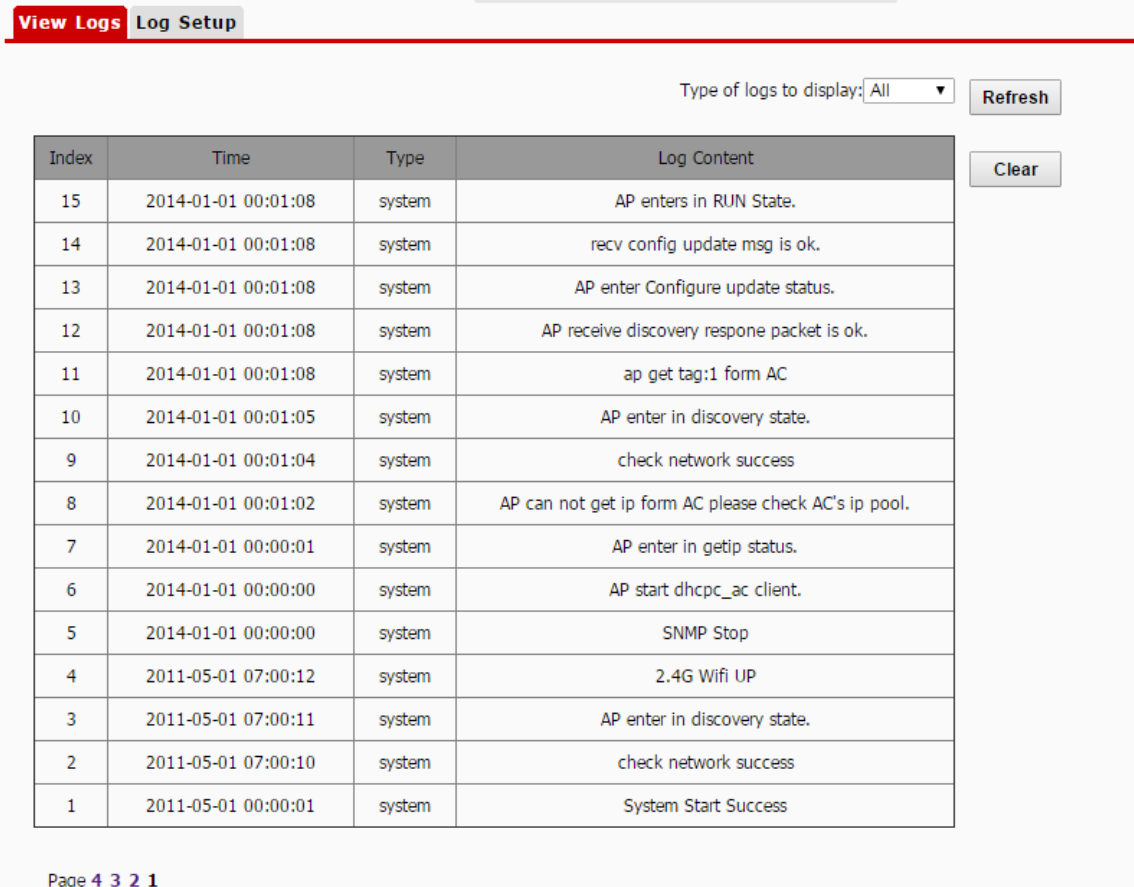
10.3 Viewing Logs

This module enables you to [view logs](#) and [configure log settings](#).

10.3.1 View Logs

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

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



The screenshot shows the 'View Logs' interface. At the top, there are two tabs: 'View Logs' (active) and 'Log Setup'. Below the tabs, there is a dropdown menu for 'Type of logs to display' set to 'All', and a 'Refresh' button. Below this is a table with the following data:

Index	Time	Type	Log Content
15	2014-01-01 00:01:08	system	AP enters in RUN State.
14	2014-01-01 00:01:08	system	recv config update msg is ok.
13	2014-01-01 00:01:08	system	AP enter Configure update status.
12	2014-01-01 00:01:08	system	AP receive discovery response packet is ok.
11	2014-01-01 00:01:08	system	ap get tag:1 form AC
10	2014-01-01 00:01:05	system	AP enter in discovery state.
9	2014-01-01 00:01:04	system	check network success
8	2014-01-01 00:01:02	system	AP can not get ip form AC please check AC's ip pool.
7	2014-01-01 00:00:01	system	AP enter in getip status.
6	2014-01-01 00:00:00	system	AP start dhcpc_ac client.
5	2014-01-01 00:00:00	system	SNMP Stop
4	2011-05-01 07:00:12	system	2.4G Wifi UP
3	2011-05-01 07:00:11	system	AP enter in discovery state.
2	2011-05-01 07:00:10	system	check network success
1	2011-05-01 00:00:01	system	System Start Success

At the bottom of the interface, there is a 'Clear' button and a page number 'Page 4 3 2 1'.

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

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

NOTE

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

10.3.2 Configuring Log Settings

To access the page, choose **Tools > Logs** and click **Log Setup**.

On this page, you can set the number of logs to be displayed and configure log servers.

The screenshot shows the 'Log Setup' page with the following elements:

- Navigation tabs: 'View Logs' and 'Log Setup' (selected).
- Number of Logs: A text input field containing '150' with a tooltip '(Default:150,Range:100~300)' and a 'Save' button.
- Enable checkbox: A checkbox labeled 'Enable' with a tooltip '(To use the following rules, you must check this box.)' and a 'Restore' button.
- Table header: A table with columns 'Index', 'Log Server IP', 'Log Server Port', 'Enable', and 'Action'.
- Buttons: 'Add' and 'Help' buttons.

Setting the Number of Logs to Be Displayed

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, choose **Tools > Logs** and click **Log Setup**.
2. Change the number of logs as required within the range of 100 to 300.
3. Click **Save**.

This screenshot is identical to the previous one, but the 'Number of Logs' input field has an asterisk (*) next to the value '150', indicating it is a required field.

---End

Configuring 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 for communicating with the log server.

Procedure for adding a log server

1. To access the page, choose **Tools > Logs** and click **Log Setup**.

2. Click **Add**.

View Logs **Log Setup**

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

Enable (To use the following rules, you must check this box.)

Index	Log Server IP	Log Server Port	Enable	Action
-------	---------------	-----------------	--------	--------

Restore Add Help

3. Set parameters as follows:

- Set **Log Server IP** to the IP address of the log server.
- Set **Log Server Port** to the UDP port number used to send and receive system logs. The default port number 514 is recommended.
- Select **Enable** to enable the log server.

4. Click **Save**.

View Logs **Log Setup**

Log Server IP Save

Log Server Port Restore

Enable Help

5. Select **Enable (To use the following rules, you must check this box.)**.

6. Click **Save**.

---End

The following figure shows the configuration.

View Logs **Log Setup**

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

Enable (To use the following rules, you must check this box.)

Index	Log Server IP	Log Server Port	Enable	Action
1	192.168.0.88	514	Enable	Edit Delete

Restore Help Add

Procedure for changing log server settings

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

---End

Procedure for deleting log server settings

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

---End

10.4 Configuration Management

This module enables you to [back up the current configuration of the AP](#), [restore a configuration of the AP](#), and [restore the factory settings of the AP](#).

10.4.1 Backing Up 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 a previous configuration.

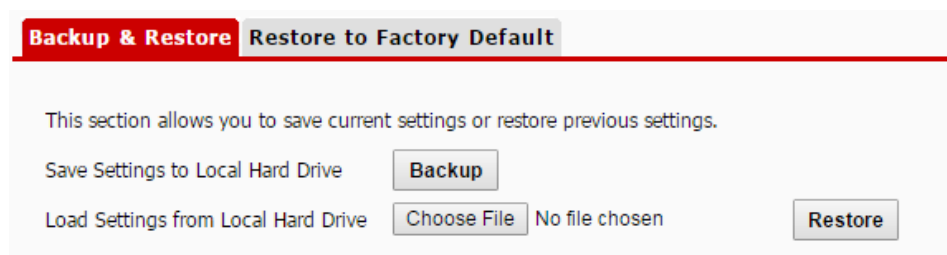
If the AP enters the optimum condition after you greatly change the configuration of the AP, you are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the AP.



If you need to apply same or similar configurations to many APs, you can configure one of the APs, back up the configuration of the AP, and use the backup to restore the configuration on the other APs. This improves configuration efficiency.

Backing Up the Current Configuration

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



---End

Restoring a Configuration

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

---End

10.4.2 Restoring the Factory Settings

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

After the factory settings are restored, the login IP address of the AP is changed to **192.168.0.254**, and the

user name and password of the AP are changed to **admin**.

 **NOTE**

- *When the factory settings are restored, your configuration is lost. Therefore, you need to reconfigure the AP to connect to the internet. Restore the factory settings of the AP only when necessary.*
- *To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.*

Restoring the Factory Settings Using Software

1. Choose **Tools > Configuration** and click the **Restore to Factory Default** tab.
2. Click the **Restore to Factory Default** button.



---End

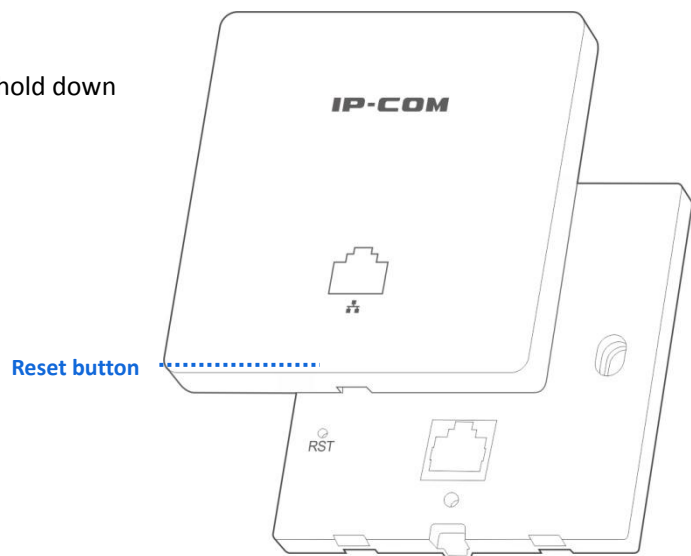
Restoring the Factory Settings Using Hardware

This method enables you to restore the factory settings without logging in to the web UI of the AP.

Procedure:

1. After the AP is powered on, use a pin to hold down the reset button for 8 seconds.
2. Wait about 1 second.

---End



10.5 Username and Password

To access page for changing user names and passwords, choose **Tools > Username & Password**.

On this page, you can change the login account information of the AP to prevent unauthorized login.

User Name & Password

Use this section to change your login user name and password.

Note: User name and password can only include 1~32 letters, numbers or underscore!

Access Mode	User Name	Enable	Action
Administrator Name	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 Mode	<ul style="list-style-type: none">■ Administrator Name: An account of this type enables you to view and modify settings of the AP.■ User: An account of this type enables you to view settings of the AP.
-------------	--

User Name	It specifies the user name of an account. By default, the AP has one administrator account and one user account. Both the user name and password of the administrator account are admin . Both the user name and password of the user account are user .
-----------	---

Enable	It specifies whether an account is enabled. <ul style="list-style-type: none">■ The administrator account is always enabled.■ The user account is enabled by default and can be disabled.
--------	--

Action	Change: This button is used to change the user name and password of the account corresponding to the button. Delete: This button is used to delete the user account. Add: This button is used to add the user account after the account is deleted.
--------	--



After changing, deleting, or adding an account, click **Save**.

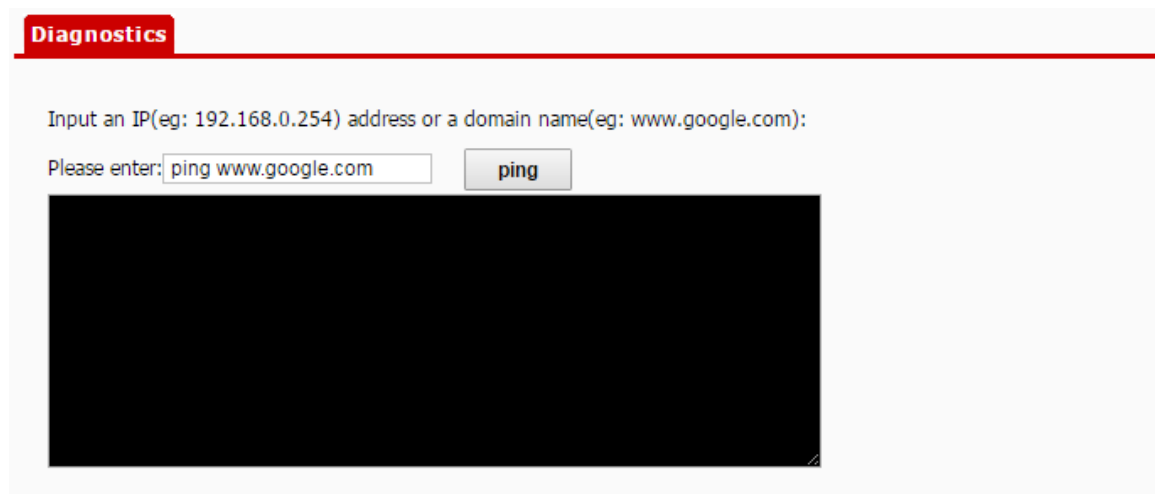
10.6 Diagnostics Tool

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

Procedure

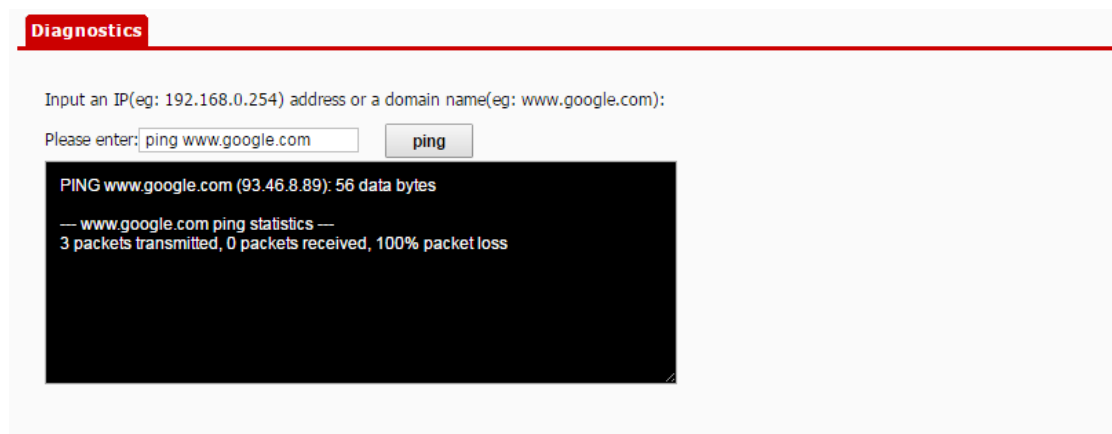
The link to www.google.com is used as an example.

1. Choose **Tools > Diagnostics**.
2. Enter the IP address or domain name to be pinged in the **Please enter** text box. In this example, enter **ping www.google.com**.
3. Click **Ping**.



---End

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



10.7 Device Reboot

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



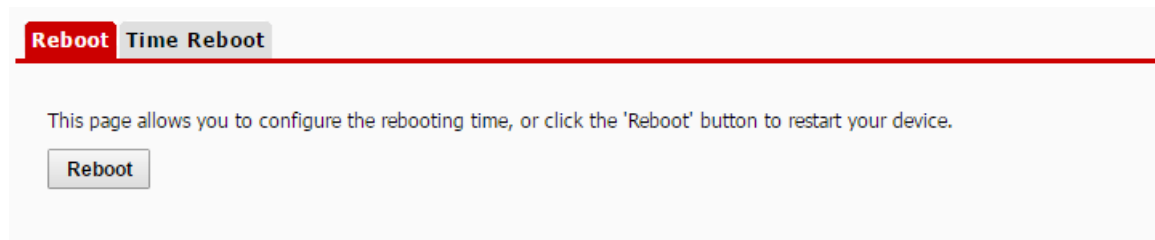
When the AP reboots, all connections are released. You are recommended to reboot the AP at an idle hour.

10.7.1 Device Reboot

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

Procedure:

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



---End

10.7.2 Time Reboot

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

- **As intervals:** In this mode, the AP reboots at the interval that you specify.
- **As Scheduled:** In this mode, the AP reboots weekly at the time that you specify.

Configuring the AP to Reboot at an Interval

1. Choose **Tools > Reboot** and click the **Time Reboot** tab.
2. Select the **Enable Auto Reboot** check box.
3. Set **AUTO Reboot Type** to **As Interval**.
4. Set **Reboot Interval** to a value in minutes, such as **1440**.
5. Click **Save**.

The screenshot shows the 'Time Reboot' configuration page. At the top, there are two tabs: 'Reboot' and 'Time Reboot', with 'Time Reboot' being the active tab. Below the tabs, there are four configuration items: 'Enable Auto Reboot' with a checked checkbox, 'AUTO Reboot Type' set to 'As Interval' in a dropdown menu, 'Reboot Interval' set to '1440' in a text box with a note '(minute,Range: 10-7200)', and three buttons: 'Save', 'Restore', and 'Help'.

---End

Configuring the AP to Reboot at Scheduled

1. Choose **Tools > Reboot** and click the **Time Reboot** tab.
2. Select the **Enable Auto Reboot** check box.
3. Set **AUTO Reboot Type** to **As Scheduled**.
4. Select the day or days when the AP reboots.
5. Set the time when the AP reboots, such as **23:59**.
6. Click **Save**.

The screenshot shows the 'Time Reboot' configuration page. At the top, there are two tabs: 'Reboot' and 'Time Reboot', with 'Time Reboot' being the active tab. Below the tabs, there are four configuration items: 'Enable Auto Reboot' with a checked checkbox, 'AUTO Reboot Type' set to 'As Scheduled' in a dropdown menu, 'Time Reboot on' with checkboxes for 'Everyday', 'Mon', 'Tue', 'Wed', 'Thur', 'Fri', 'Sat', and 'Sun', and 'Time Reboot at' set to '23:59' in a text box with a note 'eg: 23:59'. There are three buttons: 'Save', 'Restore', and 'Help'.

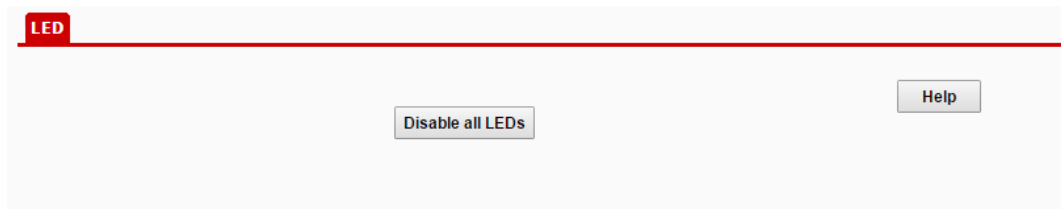
---End

10.8 LED

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

Procedure for turning off the LED indicator:

1. Choose **Tools > LED**.
2. Click **Disable all LEDs**.



---End

Procedure for turning on the LED indicator:

3. Choose **Tools > LED**.
4. Click **Enable all LEDs**.

---End

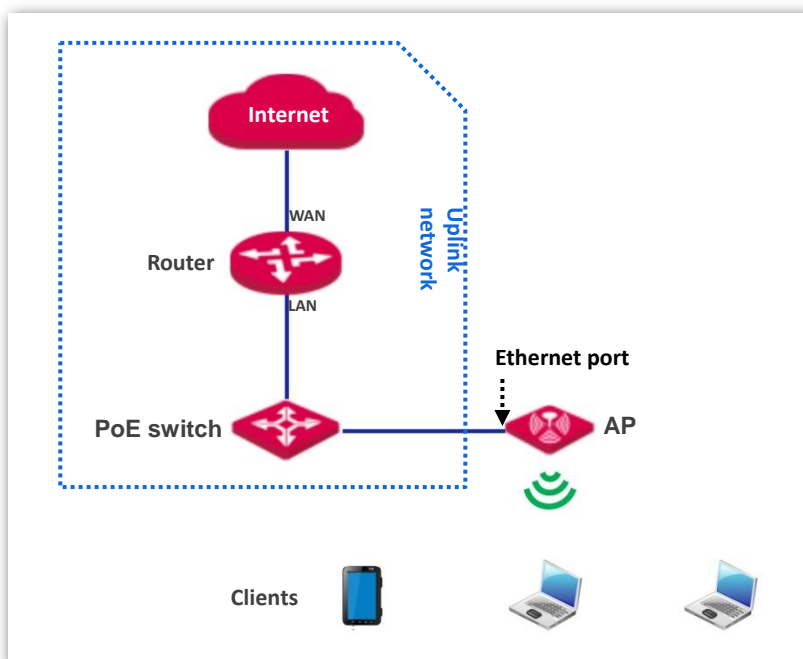
10.9 Uplink Detection

10.9.1 Overview

In AP mode, the AP connects to its upstream network using the LAN0 port. If a critical node between the LAN0 port and the upstream network fails, the AP as well as the wireless clients connected to the AP cannot access the upstream network. If uplink detection is enabled, the AP regularly pings specified hosts through the LAN0 port. If all the hosts are not reachable, the AP stops its wireless service and wireless clients cannot find the SSIDs of the AP. The client can reconnect to the AP only after the connection between the AP and the upstream networks is recovered.

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

See the following topology (The LAN0 port serves as the uplink port).



10.9.2 Configuring Uplink Detection

1. Choose **Tools > Uplink Detection**.
2. Select the **Enable** check box of **Uplink Detection**.
3. Set **Ping Host1** or **Ping Host2** to the IP address of the host to be pinged through the LAN0 port of the AP, such as the IP address of the switch or router directly connected to the AP.
4. Set **Ping Interval** to the interval at which the AP detects its uplink.
5. Click **Save**.

Uplink Detection

Uplink Detection Enable

Ping Host1

Ping Host2

Ping Interval (10 ~ 100 Minutes)

Save

Restore

Help

---End

Appendixes

FAQ

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

A1. Check the following items:

- Verify that the IP address of your computer is 192.168.0.X (X: 2~253).
- Clear the cache of your web browser or replace the web browser, and try login again.
- Disable the firewall of your computer or replace the computer, and try login again.
- If two or more APs are connected to your network without an AP controller or a router equipped with the AP controller functionality, connect one of the APs to your PoE switch and change the IP address of the AP. Repeat this procedure to connect the other APs to the PoE switch and change the IP addresses of the APs. Setting of the rest APs can be done in the same manner.
- The AP may be being managed by an AP controller and therefore its IP address is no longer 192.168.0.254. In that case, log in to the web UI of the AP controller to view the new IP address of the AP, and log in to the AP using the new IP address.
- If the problem persists, restore the factory settings of the AP and try login again.

Q2: My wireless AP controller cannot find the AP. What should I do?

A2. Check the following items:

- Verify that the devices are connected properly and the AP has started.
- If VLANs have been defined on your network, verify that the corresponding VLAN has been added to your AP controller.
- Restart the AP or restore the factory settings of the AP, and try scanning the AP again.

Q3: forget the login user name and password of the AP. What should I do to log in to the web UI of the AP?

A3. Try login with the default IP address **192.168.0.254** and default user name and password **admin**. If login fails, restore the factory settings and use the default login information to try login again.

Q4: I cannot access the web UI of the AP. What should I do to restore the factory settings?

A4. After the AP is powered on, use a pin to hold down the reset button for 8 seconds and then wait about 1 second. After the factory settings are restored, configure the AP again.

Q5: What should I do if a computer connected to the AP displays an IP address conflict message?

A5. Check the following items:

- Verify that the IP address of the computer is not used by another device on your LAN. The default IP address of the AP is 192.168.0.254.
- Verify that the static IP addresses assigned to computers on your LAN are not used by other devices.

For more technical assistance, visit our website at <http://www.ip-com.com.cn> or send your question to info@ip-com.com.cn, or call +86-755-27653089. We will help you resolve your problem as soon as possible.

Default Parameter Values

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

Parameter	Default Value	
	Management IP address	192.168.0.254
Login	User	Administrator
	Name/Password	admin admin
	User	user 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	The model of the AP. For example, the default name of W30AP V4.0 is W30APV4.0.
	Ethernet Mode	Auto-negotiation
DHCP Server	DHCP Server	Disable
	Start IP	192.168.0.100
	End IP	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 2 SSIDs. The SSID displayed is IP-COM_XXXXXX. Where XXXXXX indicates the last 6 characters of the MAC address of the LAN ports of the AP. By default, the primary SSID is enabled, and the other SSIDs are disabled.
	Broadcast SSID	Enable
	AP Isolation	Disable
	WMF	Disable
	Max. Number of Clients	16
	Chinese SSID Encoding	UTF-8
	Security Mode	None

Parameter	Default Value	
RF Status	Enable RF	Enable
	Country/Region	China
	Network Mode	11b/g/n mixed
	Channel	Auto
	Channel Bandwidth	20 MHz
	Channel Lockout	Enable
	SSID isolation	Disable
	APSD	Disable
WMM Settings	Aging Time	5 minutes
	WMM	Enable
Advanced	WMM Optimization Mode	Optimized For Capacity (10 or more)
	Beacon Interval	100 ms
	Fragment Threshold	2346
	RTS Threshold	2347
	DTIM Interval	1
	Receive Signal Strength	-90 dBm
	Power	18 dBm
	Power Lockout	Enable
Access Control	Preamble	Long Preamble
	Access Control	Disable
QVLAN	Enabled	Disable
	PVID	1
	Management VLAN	1
	Trunk Port	LAN0
	LAN Port VLAN ID	1
	2.4G SSID VLAN ID	1000
SNMP	SNMP Agent	Disable
	Administrator	Administrator
	Device Name	The model of the AP. For example, the default name of W30AP V4.0 is W30APV4.0.
	Location	ShenZhen
	Read Community	public
	Read/Write Community	private

Parameter	Default Value
Deployment	Local Deployment
Time & Date	System Time If Sync with Internet time servers is selected: Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei
	Login Timeout 5 minutes
Tools	Number of Logs Displayed 150
	Log server settings None
	Time Reboot Disable
	LED Turn On All Indicators
	Uplink Detection Disable

Safety and Emission Statement



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.

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, SHENZHEN TENDA TECHNOLOGY CO., LTD. declares that the radio equipment type W6-S is in compliance with Directive 2014/53/EU.

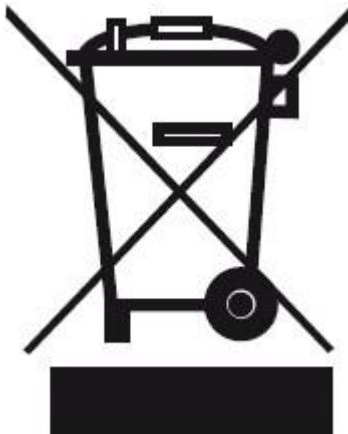
The full text of the EU declaration of conformity is available at the following internet address:

<http://www.tendacn.com/en/service/page/ce.html>

Operate Frequency: 2412-2472 MHz

EIRP Power (Max.): 19.8 dBm

Software Version: V1.0.3



RECYCLING

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 new electrical or electronic equipment.