



Wireless Access Point i9

User Guide

Copyright Statement

© 2018 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Tenda is a registered trademark legally held by Shenzhen Tenda Technology 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 Shenzhen Tenda Technology 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 Shenzhen Tenda Technology Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product 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 a warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda! Please read this user guide before you start with i9.

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: XX:XX:XX:XX:XX:XX
UI control	Bold	On the Policy page, click the OK button.
Message	<i>u </i>	The "Success" message appears.

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

Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
АР	Access Point
AC	Access Point Controller
SSID	Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ISP	Internet Service Provider
AES	Advanced Encryption Standard
VLAN	Virtual Local Area Network
ТКІР	Temporal Key Integrity Protocol

Acronym or Abbreviation	Full Spelling
РоЕ	Power Over Ethernet
WEP	Wired Equivalent Privacy

Additional information

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

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.



Contents

1 Getting to know your device1
1.1 Overview
1.2 Appearance1
1.2.1 LED indicator1
1.2.2 Button and port2
1.2.3 Label2
2 Application scenarios
2.1 Small scale WiFi network deployment4
2.1.1 Deploying the AP with a Tenda router with the AP controller capacity4
2.1.2 Deploying the AP with a router without the AP controller capacity5
2.2 Large scale WiFi network deployment6
3 Login7
3.1 Logging in to the web UI of the AP7
3.2 Logging out of the web UI of the AP9
3.3 Web UI layout9
3.4 Common buttons on the web UI10
4 Quick Setup11
4.1 Overview
4.2 Configuring AP mode13
4.3 Configuring Client+AP mode14
5 Status
5.1 System Status16
5.2 Wireless Status
5.3 Traffic Statistics19
5.4 Wireless Clients
6 Network settings
6.1 LAN setup21

	6.1.1 IP address obtaining mode – static IP address	22
	6.1.2 IP address obtaining mode – dynamic IP address	23
	6.2 DHCP server	25
	6.2.1 Overview	25
	6.2.2 Configuring the DHCP server	25
	6.2.3 DHCP clients	27
7 W	/ireless Settings	
	7.1 Basic settings	
	7.1.1 Overview	
	7.1.2 Changing the SSID setup	
	7.1.3 Examples of configuring SSID setup	35
	7.2 RF Settings	55
	7.2.1 Overview	55
	7.2.2 Changing the RF settings	55
	7.3 Channel Scan	58
	7.3.1 Overview	
	7.3.2 Checking the usage of channels	58
	7.4 WMM Setup	59
	7.4.1 Overview	59
	7.4.2 Changing the WMM settings	60
	7.5 Advanced	62
	7.5.1 Overview	62
	7.5.2 Changing the advanced settings	62
	7.6 Access Control	65
	7.6.1 Overview	65
	7.6.2 Configuring access control	65
	7.6.3 Example of configuring access control	66
	7.7 QVLAN Settings	68
	7.7.1 Overview	68
	7.7.2 Configuring the QVLAN function	68

7.7.3 Example of configuring QVLAN settings	69
8 SNMP	72
8.1 Overview	72
8.1.1 SNMP management framework	72
8.1.2 Basic SNMP operations	72
8.1.3 SNMP protocol version	73
8.1.4 MIB introduction	73
8.2 Configuring the SNMP function	74
8.3 Example of configuring the SNMP function	75
Networking requirement	75
Configuration procedure	75
Verification	76
9 Tools	77
9.1 Firmware Upgrade	77
9.2 Time & Day	78
9.2.1 System Time	78
9.2.2 Login Timeout	80
9.3 Logs	81
9.3.1 View Logs	81
9.3.2 Log settings	82
9.4 Configuration	85
9.4.1 Backup & Restore	85
9.4.2 Restoring the Factory Settings	85
9.5 Account	87
9.6 Diagnostics Tool	88
9.7 Device Reboot	90
9.7.1 Manual Reboot	90
9.7.2 Automatic Reboot	90
9.8 LED Control	92

1 Getting to know your device

1.1 Overview

Tenda i9 is a wireless access point specially designed for offices, bars, coffee shops and other indoor environments. Working at 2.4 GHz band, it provides a wireless transmission rate of as high as 300 Mbps. Featured with 2 built-in high gain omni-directional MIMO antennas, i9 provides powerful WiFi signal with strong wall penetration capacity and broad WiFi coverage. Compliant with IEEE 802.3af standard, i9 allows you to apply long-distance power supply via PoE without changing your original power network. All of this makes i9 an ideal choice for WiFi coverage.

1.2 Appearance

1.2.1 LED indicator



LED Indicator	Status	Description
	Solid on	The system is starting or faulty.
System indicator	Blinking	The system is working properly.
	Off	The system is powered off or the LED indicator is turned off.

1.2.2 Button and port



Button & Port	Connection Description
LAN port	10/100 Mbps auto negotiation port
	 If the AP is powered using a DC adapter, connect this port to a switch.
	 If the AP is powered through PoE, connect this port to an IEEE 802.3af PoE switch.
Power jack	The power jack is used to connect to a DC adapter for supplying power to the AP. Input: 12 V 1 A
Reset button	After the AP is powered on, you can hold down this button for about 8 seconds to restore the factory settings.

1.2.3 Label

The label is located on the rear panel of the AP. For details of the label, see the following figure.

	Tenda	www. tendacn.com Made in China	
	Wireless Access F	Point •	(1)
(2)	Model: i9	IP Address: 192.168.0.254	······(3)
(4)	••••••••••••••••••••••••••••••••••••••	Password: admin FCC ID: V7TI9 Part 15 of the FCC Rules. Operation is subject tions: (1) this device may not cause harmful evice must accept any interference received, may cause undesired operation.	(4)
	МАС	•	(5)
	S/N	•	(6)

- (1): Name of the AP.
- (2): Model of the AP.
- (3): Default IP address of the AP. You can use this IP address to log in to the web UI of the AP.
- (4): Default user name and password of the web UI of the AP.
- (5): MAC address of the AP. The default primary SSID of the AP is Tenda_XXXXXX, where XXXXXX indicates the last 6 characters of this MAC address.
- (6): Serial number of the AP. If the AP is faulty, you need to provide this serial number when sending the AP for repair.

2 Application scenarios

2.1 Small scale WiFi network deployment

If you need to deploy a small scale WiFi network, you are recommended to use a wired router, a PoE switch, and several APs.

2.1.1 Deploying the AP with a Tenda router with the AP controller capacity

Networking topology



- Connect the LAN port of the AP to the PoE port of the switch.
- Connect the uplink port of the switch to a LAN port of the router.
- Connect the computer used to configure APs to a LAN port of the router.

Setting up the AP

Log in to the web UI of the router, and set up the APs in batch. Refer to the user guide of the router for details.

2.1.2 Deploying the AP with a router without the AP controller capacity

If you deploy the AP with a router without the AP controller capacity, refer to the following networking topology.

Networking topology



- Connect the uplink port of the switch to a LAN port of the router.
- Connect the computer used to configure APs to the switch.
- Connect an AP to the switch first. Then perform the same procedures to connect and configure the other APs.

Setting up the AP

Log in to the web UI of the first AP, and configure it. Then configure the other APs one by one.

Refer to <u>Chapter 3</u> and the follows in this user guide for details.



If multiple APs are needed to setup, change their IP addresses to different ones to avoid IP conflict.

2.2 Large scale WiFi network deployment

If you need to deploy a large scale WiFi network in hotels, enterprises, or stations, you are recommended to use a wired router, a PoE switch, a Tenda AP controller, and several APs.

Networking topology



- Connect the computer used to configure APs to the Tenda AP controller.
- Connect the LAN port of the AP to the PoE port of the switch.

Setting up the AP

Log in to the web UI of the Tenda AP controller, and set up the APs in batch. Refer to the user guide of the Tenda AP controller for details.



3.1 Logging in to the web UI of the AP

- **Step 1** Connect the computer to the AP or the switch connected to the AP.
- **Step 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**.

Internet Protocol Version 4 (TCP/IPv4)	Properties 🔹 💦 💌
General	
You can get IP settings assigned auton this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator
Obtain an IP address automatical	y
• Use the following IP address:	
IP address:	192.168.0.10
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
Default gateway:	
Obtain DNS server address autom	natically
O Use the following DNS server add	resses:
Preferred DNS server:	
<u>A</u> lternate DNS server:	· · ·
Vajidate settings upon exit	Ad <u>v</u> anced
	OK Cancel

Step 3 Access 192.168.0.254 using a web browser.



Step 4 Enter **admin** as the user name and password and click **Login**.

Default user name: admin Default password: admin
English •
Login
Forget your password?

₽TIP

If this page is not displayed, refer to <u>Q1</u> in Appendix A "FAQ".

--End

You can now start configuring the AP.

∿	Status	System Status	
	System Status		
	Wireless Status	System Status	Неір
	Traffic Statistics	AP Name	i9V2.0
	Wireless Clients	System Time	2018-11-02 11:18:39
\$	Quick Setup	Uptime	00h00m45s
	Network	Number of Clients	0
(i:	Wireless	Firmware Version	V1.0.0.6(1020)
*	SNMP	Hardware Version	V2.0
-	🖏 Tools	LAN Status	
~0~		MAC Address	C8:3A:35:83:EF:D0
		IP Address	192.168.0.254
		Subnet Mask	255.255.255.0
		Primary DNS Server	192.168.0.252
		Secondary DNS Server	8.8.8.8

3.2 Logging out of the web UI of the AP

After you log in to the web UI of the AP, the system logs you out if you perform no operation on the web UI within the <u>Login Timeout</u> interval. (The default interval is 5 minutes and can be changed.)

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

When you are logged out, the system does not save the current configuration. Therefore, you are recommended to save the current configuration before logging out.

₽ TIP

If you close the web browser tab page used to log in to the web UI of the AP instead of the web browser, you are not logged out.

3.3 Web UI layout

The web UI of the AP is composed of 4 parts, including the level-1 navigation tree, level-2 navigation tree, tab page area, and configuration area. See the following figure.

 ₩TIF

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.

.∿	Status 1	System Status	
	System Status	System Status	Help
2	Wireless Status	oyotan otatao	
	Traffic Statistics	AP Name	i9V2.0
	Wireless Clients	System Time	2018-11-02 11:18:39
4	Quick Setup	Uptime	00h00m45s
۲	Network	Number of Clients	0 4
(¢	Wireless	Firmware Version	V1.0.0.6(1020)
*	SNMP	Hardware Version	V2.0
ö.	Tools	LAN Status	
~o	10013	MAC Address	C8:3A:35:83:EF:D0
		IP Address	192.168.0.254
		Subnet Mask	255.255.255.0
		Primary DNS Server	192.168.0.252
		Secondary DNS Server	8.8.8.8

No.	Name	Description
1	Level-1 navigation tree	The powerstion have display the function many of the AD. When
2	Level-2 navigation tree	you select a function in navigation bar, the configuration of the
3	Tab page area	
4	Configuration area	It enables you to view and modify configuration.

3.4 Common buttons on the web UI

Description of common buttons:

Button	Description
Refresh	It is used to update the content of the current page.
Save	It is used to save the configuration on the current page and enable the configuration to take effect.
Restore	It is used to change the current configuration on the current page back to the original configuration.
Help	It is used to view help information corresponding to the settings on the current page.



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 <u>AP</u> or <u>Client+AP</u> 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.



Client+AP mode

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



4.2 Configuring AP mode

The Mixed WPA/WPA2-PSK security mode and AES encryption algorithm are used as an example to describe the configuration procedure. If you need to use another security mode, refer to Section <u>7.1 Basic settings</u>.

Configuration procedure:

- **Step 1** Set **Working Mode** to **AP**.
- **Step 2** (Optional) Set **SSID** to a wireless network name.
- **Step 3** Set **Security Mode** to **Mixed WPA/WPA2-PSK**, **Encryption Algorithm** to **AES**, and **Key** to the password of the wireless network.

Step 4 Click **Save**.

Quick Setup		
Working Mode	AP Client+AP	Save
SSID	Tenda_888888	Restore
Security Mode	Mixed WPA/WPA2-PSK	
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES	Help
Key	••••••	

--End

Parameter description

Parameter	Description
Working Mode	It specifies the working mode of the AP, including AP mode and Client+AP mode.
SSID	It specifies the primary SSID (wireless network name) of the wireless network at the corresponding radio band.
Security Mode	It specifies the security mode of the wireless network, including: 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.

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.

4.3 Configuring Client+AP mode

Configuration procedure:

₽TIP

Before configuration, ensure that the upstream AP is connected to the internet successfully.

Assume that the upstream AP has the basic information described in the following table.

IP Address	SSID	Security Mode	Security Key (Wireless Network Password)
192.168.0.254	Tenda_1	WPA2-PSK	87654321

- Step 1 Log in to the web UI of this AP, and change its IP address to an unused IP address belonging to the same network segment as that of the upstream AP, such as 192.168.0.253. For details, refer to Section <u>6.1 LAN Setup</u>.
- **Step 2** Use the new IP address to log in to the web UI of this AP, and choose **Quick Setup**.
- **Step 3** Set the **Working Mode** to **Client+AP**.
- Step 4 Click Scan.
- **Step 5** Select the SSID of the upstream AP from the detected SSIDs, which is **Tenda_1** in this example.

. ₽TIF

If the AP detects no wireless network, choose **Wireless** > **Basic** to enable the wireless function, and then try again.

- Step 6 After you select an SSID, the SSID, Security Mode, Encryption Algorithm, and Upstream AP Channel are populated automatically. You just need to enter the password of the wireless network of the upstream AP in the Key box. Set Key to the wireless network password of the upstream AP, which is 87654321 in this example.
- **Step 7** Click **Save**.

Quic	k Setup							
	Working M	ode	🔵 AP 💿 Clie	ent+AP				Save
	S	SSID Tenda_1					Restore	
	Security Mode		WPA2-PSK		•			
	Encryption Algorithm		AES T	KIP 🔘 TKIP	&AES			Help
	Key		•••••					
	Upstream AP Channel		11		•			
			D	isable Scan				
Select	SSID	MA	C Address	Network Mode	Channel Bandwidth	Channel	Extension Channel	Security Mode
۲	Tenda_1	50:2b	:73:09:94:51	bgn	40	11	upper	wpa2/aes

--End

Parameter description

Parameter	Description
Working Mode	It specifies the working mode of the AP, including AP Mode and Client+AP Mode.
SSID	It specifies the SSID (wireless network name) of the upstream AP to be bridged. It is populated automatically when you select the SSID of the upstream AP.
Security Mode	It specifies the security mode of the wireless network to be bridged. The AP can bridge to a wireless network using None, WEP (Open or shared), WPA-PSK, WPA2-PSK, or Mixed WPA/WPA2-PSK security mode. Clicking the hyperlink navigates you to the elaborated description of the corresponding security mode.
Authentication Type	It specifies the WEP authentication type of the wireless network to be bridged. It needs to be manually entered.
Default Key	It specifies the WEP default key (wireless password) of the wireless network to be bridged. It needs to be manually entered.
WEP Key 1 to 4	It specifies the WEP key of the wireless network to be bridged. It needs to be manually entered.
Encryption Algorithm	It specifies the WPA cipher type of the wireless network to be bridged. It is populated automatically when you select the SSID of the upstream AP.
Кеу	It specifies the wireless password of the wireless network to be bridged. It needs to be manually entered.
Upstream AP Channel	It specifies the wireless channel used by the upstream AP. It is populated automatically when you select the SSID of the upstream AP.

After the settings take effect, use your smart phone to search the SSID of this AP, and enter the key for internet access. Choose **Wireless** > **Basic** to check or change the SSID and key.



5.1 System Status

To view the system status and LAN status of the AP, choose **Status** > **System Status**.

System Status		
System Status	Help	
AP Name	i9V2.0	
System Time	2018-11-02 11:18:39	
Uptime	00h00m45s	
Number of Clients	0	
Firmware Version	V1.0.0.6(1020)	
Hardware Version	V2.0	
LAN Status		
MAC Address	C8:3A:35:83:EF:D0	
IP Address	192.168.0.254	
Subnet Mask	255.255.255.0	
Primary DNS Server	192.168.0.252	
Secondary DNS Server	8.8.8	

Parameter description

Parameter	Description
	It specifies the name of the AP.
AP Name	A unique Device Name helps quickly identify the AP. You can change the Device Name on the Network > LAN Setup page.
System Time	It specifies the current system time of the AP.
Uptime	It specifies the time that has elapsed since the AP was started last time.
Number of Clients	It specifies the number of wireless clients currently connected to the AP.
Firmware Version	It specifies the firmware version number of the AP.

Parameter	Description
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.
	It specifies the IP address of the AP.
IP Address	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 secondary DNS server of the AP.

5.2 Wireless Status

To view the radio status and SSID status of the wireless network, choose **Status** > **Wireless Status**.

/ireless Status					
	RF S	tatus			Help
RF (On/Off)	RF (On/Off)				
Network Mode	Network Mode		b/g/n		
Channel	Channel		4		
	SSID	Status]
SSID	MAC A	ddress	Enabled/Disabled	Security Mode	
Tenda_1	C8:3A:35	:83:EF:D1	Enabled	WPA2-PSK	
Tenda_83EFD1	C8:3A:35:83:EF:D2		Disabled	None	
Tenda_83EFD2	C8:3A:35	:83:EF:D3	Disabled	None	
Tenda_83EFD3	C8:3A:35	:83:EF:D4	Disabled	None	

Parameter description

Parameter		Description
	RF (On/Off)	It specifies whether the wireless function of the AP is enabled.
RF Status	Network Mode	It specifies the current network mode of the AP.
	Channel	It specifies the current working channel of the AP.
	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.
SSID Status	Enable/Disable	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 view the total transmitted traffic, total received traffic, total number of transmitted packets, and total number of received packets corresponding to each SSID of the AP, choose **Status** > **Traffic Statistics**.

c Statistics					
SSID	Received Traffic	Received Packets	Transmitted Traffic	Transmitted Packets	Help
Tenda_1	22.78MB	105400	0.38MB	1667	Refree
Tenda_888889	0.00MB	0	0.00MB	0	
Tenda_88888A	0.00MB	0	0.00MB	0	
Tenda_88888B	0.00MB	0	0.00MB	0	

You can click **Refresh** to view the latest traffic statistics.

5.4 Wireless Clients

To view the MAC address, IP address, connection uptime, transmit speed, and receive speed of each wireless client connected to the AP, choose **Status** > **Wireless Clients**.

Vireless	<u>Clients</u>					
You can vie	w information about the wir	eless devices that are c	connected to the	wireless networks	of the AP.	Help
Connected	Hosts:		Ter	nda_888888	v	
			Connection	Transmit		
ID	MAC Address	IP	Connection Uptime	Transmit Speed	Receive Speed	

You can select an SSID from the drop-down list box in the upper-right corner to view information about the wireless clients connected to the AP using the SSID.



6.1 LAN setup

To view or configure the MAC address, device name, IP address obtaining mode, and other related information of the LAN port of the AP, choose **Network** > **LAN Setup**.

LAN Setup			
MAC Address	C8:3A:35:83:EF:D0		Save
IP Address Type	Static •]	Restore
IP Address	192.168.0.254	Example: 192.168.1.254	
Subnet Mask	255.255.255.0	Example: 255.255.255.0	Help
Gateway	192.168.0.1		
Primary DNS Server	8.8.8.8]	
Secondary DNS Server		(optional)	
AP Name	i9V2.0]	
Driving Capability of Port	●Standard ○Enhanced (lower port sp	eed)	

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 Tenda_XXXXXX, where XXXXXX indicates the last
	It specifies the IP address obtaining mode of the AP. The default option is Static IP .
	 Static: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is set manually.
IP Address Type	• Dynamic : It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP is obtained from a DHCP server in your LAN.
	If IP Address Type is set to Dynamic , 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 if IP Address Type is set to Static . The default IP address is 192.168.0.254 and you can change it as required.

Parameter	Description
	C NOTE This IP address also functions as the management IP address of the AP. You can use this IP address to log in to the web UI of the AP to manage the AP.
Subnet Mask	It specifies the subnet mask of the IP address of the AP if IP Address Type is set to Static . The default subnet mask is 255.255.255.0 and you can change it as required.
Gateway	It specifies the gateway of the AP if IP Address Type is set to Static . The default gateway IP address is 192.168.0.1 and you can change it as required.
Primary DNS Server	It specifies the primary DNS server of the AP if IP Address Type is set to Static . The default IP address of the primary DNS server is 8.8.8.8 and you can change it as required.
Secondary DNS Server	It specifies the secondary DNS server of the AP if IP Address Type is set to Static . This IP address is optional.
	It specifies the device name of the AP. The default device name is in the format of <i>Model</i> + <i>Hardware version number</i> .
Ar Name	You are recommended to change the device name so that you can quickly locate the AP when managing the AP remotely.
	It specifies the Ethernet mode of LAN of this AP.
	• Standard : This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended.
Driving Capability of Port	• Enhanced (lower port speed): This mode features a long transmission distance but relatively low transmission rate (10 Mbps).
	This mode is recommended only if the Ethernet cable that connects the LAN port of the AP to a peer device exceeds 100 meters. In this case, the connected LAN port of the peer device must work in auto-negotiation mode. Otherwise, the LAN port of the AP may not be able to properly transmit or receive data.

If you change the IP address of the LAN port, change the IP address of your management computer as well so that the two IP addresses belong to the same network segment. Then, use the new IP address of the LAN port to log in to the web UI of the AP.

6.1.1 IP address obtaining mode – static IP address

This mode enables you to set the IP address, subnet mask, gateway IP address, primary DNS server, and secondary DNS server of the AP. It is applicable to a scenario with only one or a few APs.

Configuration procedure:

- **Step 1** Set **IP Address Type** to **Static**.
- **Step 2** Set **IP Address**.
- **Step 3** Set **Subnet Mask** to the subnet mask of the IP address. Generally the subnet mask is 255.255.255.0.
- **Step 4** Set **Gateway** to the IP address of the gateway of the AP.
- **Step 5** Set **Primary DNS Server** to the IP address of the primary DNS server of the AP. If another DNS server is available, set **Secondary DNS Server** to the IP address of the additional DNS server.
- Step 6 Click Save.

LAN Setup			
MAC Address	C8:3A:35:83:EF:D0		Save
IP Address Type	Static	T	Restore
IP Address	192.168.0.254	Example: 192.168.1.254	
Subnet Mask	255.255.255.0	Example: 255.255.255.0	Help
Gateway	192.168.0.1		
Primary DNS Server	8.8.8.8		
Secondary DNS Server		(optional)	
AP Name	i9V2.0		
Driving Capability of Port	Standard DEnhanced (lower)	port speed)	

--End

6.1.2 IP address obtaining mode – dynamic IP address

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

Configuration procedure:

- **Step 1** Set **IP Address Type** to **Dynamic**.
- Step 2 Click Save.

LAN Setup		
MAC Address	C8:3A:35:83:EF:D0	Save
IP Address Type	Dynamic 🔻	Restore
AP Name	i9V2.0	
Driving Capability of Port	●Standard ○Enhanced (lower port speed)	Help

--End

6.2 DHCP server

6.2.1 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.

6.2.2 Configuring the DHCP server

- **Step 1** Select the **Enable** check box of **DHCP Server**.
- **Step 2** Set **Start IP Address** to the start IP address of the IP address pool, which contains the IP addresses that can be assigned by the DHCP server to clients.
- Step 3 Set End IP Address to the end IP address of the IP address pool.
- Step 4 Set Lease Time to the time when an IP address is available to a client. The default option 1 day is recommended.
- **Step 5** Set **Subnet Mask** to the subnet mask of the IP addresses. The default value **255.255.255.0** is recommended.
- **Step 6** Set **Gateway** to the gateway IP address to be assigned by the DHCP server to clients.
- Step 7 Set Primary DNS Server to the IP address of the primary DNS server assigned by the DHCP server to clients. If another DNS server IP address is available, set Secondary DNS Server to that IP address.
- Step 8 Click Save.

DHCP Server DHCP Clie	ents	
DHCP Server	🕑 Enable	Save
Start IP Address	192.168.0.100	Restore
End IP Address	192.168.0.200	
Lease Time	1 day	т
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	(optional)

--End

Parameter description

Parameter	Description
DHCP Server	It specifies whether to enable the DHCP server function. To enable it, select the check box. To disable it, deselect the check box. By default, it is disabled.
Start IP Address	It specifies the first IP address that can be assigned by the DHCP server to a client. The default value is 192.168.0.100 .
End IP Address	It specifies the last IP address that can be assigned by the DHCP server to a client. The default value is 192.168.0.200 .
Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a client. The default value is 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 gateway IP address assigned by the DHCP server to clients. The default value is 192.168.0.1 . Image: Note When a client accesses a server or host located outside the network segment where the client resides, the data from and to the client must be forwarded by the gateway. Generally, the IP address of the gateway is the LAN IP address of the router in your LAN.
Primary DNS Server	It specifies the primary DNS server IP address assigned by the DHCP server to clients. The default value is 8.8.8.8 . IDENOTE To enable clients to access web pages using domain names, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS Server	It specifies the secondary DNS server IP address assigned by the DHCP server to clients. This IP address is optional.

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

6.2.3 DHCP clients

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 view information about the clients that obtain IP addresses from the DHCP server function of the AP, choose **Network > DHCP Server** and click the **DHCP Clients** tab.

DHCP Server DHCP Clients					
If the DHCP	If the DHCP server is enabled, the client list is updated every five seconds.				
ID	ID Host Name IP Address MAC Address Lea				
1	iPhone	192.168.0.133	1c:5c:f2:b4:40:08	23:59:53	

You can click **Refresh** to view the latest client information.



7.1 Basic settings

This module enables you to set SSID-related parameters of wireless networks of your AP.

7.1.1 Overview

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.

Isolate Client

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 IEEE 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 SSID setup

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

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

Basic			
* SSID	Tenda_888888	•	Save
* Enable	✓		Restore
Broadcast SSID	Enable	•	
Isolate Client	Disable Disable		Help
WMF	Disable Disable		
Max. Number of Clients	48	(Range: 1 - 64)	
* SSID	Tenda_888888		
Chinese SSID Encoding	UTF-8	•	
* Security Mode	Mixed WPA/WPA2-PSK	•	
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES		
Key	•••••		
Key Update Interval	0		
	(Range: 0 or 60 - 99999; 0: not to update)		

--End

Parameter	Description
	It specifies the SSID to be configured.
SSID	The AP allows 4 SSIDs. The default SSID is the primary SSID of the AP, which is Tenda_XXXXXX, where XXXXXX indicates the last 6 characters in the MAC address specified on the label on the external surface of the AP.
Enable	It specifies whether to enable the selected SSID.
	By default, the primary SSID is enabled and the other SSIDs are disabled. You can enable them as required.

Parameter	Description
	It specifies whether to broadcast the selected SSID.
	 Enable: It indicates that the AP broadcasts the SSID and the SSID can be detected by clients.
Broadcast SSID	• Disable : It indicates that the AP does not broadcast the SSID and the SSID cannot be detected by clients. If a user wants to connect to the wireless network corresponding to this SSID, the user must enter the SSID manually.
	This AP can automatically hide its SSID. When the number of clients connected to the AP with an SSID of the AP reaches the <u>Maximum Clients</u> , the AP stops broadcasting the SSID.
	It specifies whether to isolate the wireless clients connected to the AP with the selected SSID.
Isolate Client	• 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.
WMF	It specifies whether to forward multicast packets through unicast tunnels. Generally, multicast packets are usually transmitted at the lowest rate, such as 1 Mbps, leading to poor transmission efficiency. WMF leverages the high auto-negotiated rate, reliable feedback mechanism, and other advantages of unicast packets to address multicast problems such as video playback stalls caused by packet loss and long delays over a wireless network.
Max. Number of	It specifies the maximum number of wireless clients that can connect to the AP with the selected SSID.
Cheffes	After this upper limit is reached, the AP rejects new connection requests from clients.
SSID	It enables you to change the selected SSID. Chinese characters are allowed in an SSID.
Chinasa SSID	It specifies the encoding format of Chinese characters in an SSID. The default value is UTF8 .
Encoding	If 2 or more SSIDs of the AP are enabled, you are recommended to set this parameter to UTF-8 for some SSIDs and to GB2312 for the other SSIDs, so that any wireless client can identify one or both SSIDs that contain Chinese characters.
Security Mode	It specifies the encryption type of the selected SSID. None indicates that any wireless client can connect to the AP using the selected SSID. This option is not recommended because it affects network security.
	The AP supports the WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2 security modes, which are elaborated in the following section.

None

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

WEP

Security Mode	WEP v	
Authentication Type	Open 🔻	
Default Key	Open Shared	
Key 1	802.1x 12345	ASCII 🔻
Key 2	12345	ASCII V
Key 3	12345	ASCII V
Key 4	12345	ASCII 🔻

Parameter	Description
	It specifies the encryption type for the WEP security mode of the AP. The options include Open , Shared , and 802.1x .
	The options share the same encryption process.
	• Open
Authentication Type	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
	It specifies that 802.1x authentication is required and data exchanged is encrypted 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 default WEP key for the Open and Shared encryption types.
,	For example, if Default Key is set to Key 2 , a wireless client can connect to the

Parameter	Description	
	wireless network corresponding to the selected SSID only with the password specified by 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	
RADIUS Port	It specifies the IP address/port number/shared key of the RADIUS server for	
RADIUS Password	authentication.	

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

Security Mode	WPA-PSK •
Encryption Algorithm	None WEP
Key	WPA-PSK WPA2-PSK
Key Update Interval	Mixed WPA/WPA2-PSK WPA
	(Range: 0 or 60 - 99999; 0: not to
	update)

Parameter	Description
Security Mode	It indicates the personal or pre-shared key security mode, including WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK.
	• 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.
Encryption Algorithm	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.
	• AES: It indicates the Advanced Encryption Standard.

Parameter	Description
	• 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.
Кеу	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

Security Mode	WPA 🔻	
RADIUS Server IP	None WEP	
RADIUS Port	WPA-PSK WPA2-PSK Mixed WPA/WPA2-PSK	(Range: 1025 - 65535; Default: 1812)
RADIUS Password	WPA WPA2	
Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES	
Key Update Interval	0	
	(Range: 0 or 60 - 99999; 0: not to update)	

Parameter	Description
Security Mode	 The WPA and WPA2 options are available for network protection with a RADIUS server. 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.
Encryption Algorithm	 It specifies the encryption algorithm corresponding to the selected security mode. The available options include AES, TKIP, and TKIP&AES. AES: It indicates the Advanced Encryption Standard. TKIP: It indicates the Temporal Key Integrity Protocol.

Parameter	Description
	 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 SSID setup

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.

- **Step 1** Choose **Wireless** > **Basic**.
- **Step 2** Select the second SSID from the SSID drop-down list box.
- **Step 3** Select the **Enable** check box.
- **Step 4** Change the value of the SSID text box to **FREE**.
- **Step 5** Set **Security Mode** to **None**.

sic			
* SSID	FREE	Ŧ	Save
* Enable			Restor
Broadcast SSID	Enable	T	
Isolate Client	Disable Disable		Help
WMF	Disable Disable		
Max. Number of Clients	48	(Range: 1 - 64)	
* SSID	FREE		
Chinese SSID Encoding	UTF-8	Ŧ	
* Security Mode	None	T	

--End

Step 6 Click **Save**.

Verification

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

Setting up a wireless network encrypted using WPA/WPA2-PSK

Network requirement

A company 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.



Configuration procedure:

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

- **Step 1** Choose **Wireless** > **Basic**.
- **Step 2** Select the second SSID from the SSID drop-down list box.
- **Step 3** Select the **Enable** check box.
- **Step 4** Change the value of the **SSID** text box to **Hotspot**.
- **Step 5** Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.
- **Step 6** Set **Key** to **87654321**.
- Step 7 Click Save.

Basic				
* SSID	Hotspot	•		Save
≭ Enable	1			Restore
Broadcast SSID	Enable	•		
Isolate Client	Disable Disable			Help
WMF	Disable Disable			
Max. Number of Clients	48	(Ra	ange: 1 - 64)	
* SSID	Hotspot			
Chinese SSID Encoding	UTF-8	•		
\star Security Mode	WPA2-PSK	•		
* Encryption Algorithm	● AES ○ TKIP ○ TKIP&AES			
* Key	•••••			
Key Update Interval	0			
	(Range: 0 or 60 - 99999; 0: not to update)			

--End

Verification

Wireless devices can connect to the **Hotspot** wireless network with the password **87654321**.

Setting up a wireless network encrypted using WPA or WPA2

Network requirement

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



Configuration procedure:

Configuring the AP

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

Assume that the second SSID of the AP is used.

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

Basic			
* SSID	hot_spot •]	Save
* Enable	Ø		Restore
Broadcast SSID	Enable •]	
Isolate Client	Disable Disable		Help
WMF	Disable		
Max. Number of Clients	48	(Range: 1 - 64)	
* SSID	hot_spot]	
Chinese SSID Encoding	UTF-8]	
★ Security Mode	WPA2 v]	
* RADIUS Server IP	192.168.0.200]	
* RADIUS Port	1812	(Range: 1025 - 65535; Default: 1812)	
* RADIUS Password	••••••]	
* Encryption Algorithm	● AES		
Key Update Interval	0]	

--End

Configuring the RADIUS server

₽TIP

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

Step 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**.

🐤 Internet Authenti	cation Service			_ 🗆	×
<u>F</u> ile <u>A</u> ction <u>V</u> iew	<u>H</u> elp				
← → 🗈 💽	🖥 🛃 😫				
👳 Internet Authenticat	ion Service (Local)	Frier	ndly Name	Address	
RADIUS Clients	New RADIUS <u>C</u> lie	nt I	There are no item	ns to show in this view.	
Remote Access	<u>N</u> ew	•			
🦉 Connection	⊻iew	•			
Hemote HA	Re <u>f</u> resh Export <u>L</u> ist				
	<u>H</u> elp				
					Þ
New Client					

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

Type a friendly name and	l either an IP Address or DNS name for the client.
Eriendly name:	root
Client address (IP or DNS	i):
IP address of	your AP
IP address of	your AP

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

Nev	RADIUS Client		×
	Additional Information		
	If you are using remote access policies vendor of the RADIUS client. Client-Vendor:	based on the client vendor attribute, specify the	1
	RADIUS Standard	_	
	Shared secret:	******	
	Confirm shared secret:	******	
	<u>B</u> equest must contain the Message	ge Authenticator attribute	
	Passwo	rd same as that specified	
	by RAD	IUS Password on the AP	
		< Back Finish Cancel	

Step 2 Configure a remote access policy.

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

la Antian Minus Hala			
le Action View Help	and the second secon		
• -> 🗈 🖪 🐼 🗟	3		
Internet Authentication Servic	e (Local)	Name	Order
RADIUS Clients		S Connections to Microsoft Routing and Remote A	1
Remote Access Logging		Connections to other access servers	2
Connection Request Pr	New Remote Access P	olicy	
	New	*	
	 ⊻iew		
	- Defeat		
	Fiegresh Evport List		
1.	Export From		
	<u>H</u> elp		

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

To continue, click Next.	ile Action New Remote Access Policy V → → RADIL → Remo Remo © Remo	Wizard Welcome to the New Remote Access Policy Wizard This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.
< Back. Next> Cancel		To continue, click Next.
		Cancel

42

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

New Remote Access Policy Wizard
Policy Configuration Method The wizard can create a typical policy, or you can create a custom policy.
How do you want to set up this policy?
Use the wizard to set up a typical policy for a common scenario
Set up a custom policy
Type a name that describes this policy.
Policy name: root
Example: Authenticate all VPN connections.
< <u>B</u> ack <u>N</u> ext > Cancel

Select Ethernet and click Next.

lew	Remote Access Policy Wizard
^	CCESS Method Policy conditions are based on the method used to gain access to the network.
	Select the method of access for which you want to create a policy.
	Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
	C <u>D</u> ial-up
	Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
	C <u>W</u> ireless
	Use for wireless LAN connections only.
	 Ethernet Use for Ethernet connections, such as connections that use a switch.
	< <u>B</u> ack Next> Cancel

Select Group and click Add.

User or Group Access	A
You can grant access to individual us groups.	ers, or you can grant access to selected
Grant access based on the following:	
C User	
User access permissions are specifie	ed in the user account.
Group name:	Add <u>B</u> emove

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

	Object Types
	Locations
	<u>C</u> heck Names
ОК	Cancel

Select Protected EAP (PEAP) and click Next.

Authentication Methods	es la sulhantiasta	10000	ŕ
EMP uses different types of security devic	es to admenticate	users.	l
Select the EAP type for this policy.			
<u>I</u> ype:			
Protected EAP (PEAP)		▼ Cor	nfigure

Click Finish. The remote access policy is created.

New Remote Access Policy W	izard	X
6	Completing the New Remote Access Policy Wizard	
V	You have successfully completed the New Remote Access Policy Wizard. You created the following policy:	
	root	
	Conditions: NAS-Port-Type matches ''Ethernet'' AND Windows-Groups matches "COMBA\802.1x"	
	Authentication: EAP(Protected EAP (PEAP))	
	Encryption: Basic, Strong, Strongest, No encryption	
	To close this wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	

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

root Properties	? ×
Settings	
- 1	1
Specify the conditions that connection requests mus	: match.
Policy <u>c</u> onditions:	
NAS-Port-Type matches "Ethernet" AND Windows-Groups matches "COMBA/802.1x"	
Add Edit Bemove	
	tin this setting the
associated profile will be applied to the connection.	a in this policy, the
E-dit Profile	
Unless individual access permissions are specified in policy controls access to the network.	the user profile, this
If a connection request matches the specified condition O Denv remote access permission	ions:
Grant remote access permission	
	ncel Apply

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

NAS-Port-Type	? ×
Available types:	Selected types:
PIAFS SDSL - Symmetric DSL Sync (T1 Line) Token Ring Virtual (VPN) Wireless - IEEE 802.11 Wireless - Other X.25 X.75 xDSL - Digital Subscrib	Ethernet Wireless - IEEE 802.11
	OK Cancel

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

DiaLin Constraints) IP	1 Multilisk
Authentication	Encryption	Advanced
elect the authentication m	ethods you want to allow) for this connection.
Microsoft Encrypted A	Authentication version $\underline{2}$ ge password after it has	(MS-CHAP v2) expired
Microsoft Encrypted A	Authentication (MS-CHAF	P)
User can chan	ge password after it has	expired
Encrypted authentica	tion (CHAP)	
Unencrypted authenti	ication (PAP, SPAP)	
Unauthenticated access		
Allow clients to conne method.	ect without negotiating a	n authentication

When a message appears, click No.

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

--End

Configure your wireless device

₽TIP

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

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



Step 2 Click Add.



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



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

Manually connect	to a wireless network	
Enter information	n for the wireless network you w	ant to add
Network name:	hot_spot	
Security type:	WPA2-Enterprise	Same as the security mode
Encryption type:	AES -	of the WiFi network of the AP
Security Key:		Hide characters
✓ Start this conne ✓ Connect even if Warning: If you	ction automatically the network is not broadcasting select this option, your computer's privad	y might be at risk.
		Next Cancel



(A) at	Manually connect to a wireless network	- • •
	manually connect to a whereas network	
Su	ccessfully added hot_spot	
f		
	 Change connection settings Open the connection properties so that I can change the settings. 	
÷		.;
		Close

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

hot_spot Wireless Netwo	ork Properties
Connection Security	
	,
Security type:	WPA2-Enterprise 🔻
Encryption type:	AES 💌
Choose a network aut Microsoft: Protected I Remember my creatine I'm logged on Advanced settings	hentication method: EAP (PEAP) Settings dentials for this connection each
	OK Cancel

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

Protected EAP Properties
When connecting:
<u>Nalidate server certificate</u>
Connect to these servers:
Trusted <u>R</u> oot Certification Authorities:
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
🔲 GlobalSign Root CA 🔤
Microsoft Root Authority
Microsoft Root Certificate Authority
Microsoft Root Certificate Authority 2011
Thawte Timestamping CA
◄
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
📝 Enable <u>F</u> ast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK Cancel

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



Step 9 Click **Advanced settings**.

hot_spot Wireless Netw	ork Properties	×
Connection Security		
S <u>e</u> curity type: E <u>n</u> cryption type:	WPA2-Enterprise	
Choose a network au Microsoft: Protected V Remember my cre time I'm logged on	thentication method: EAP (PEAP) dentials for this connection each	
A <u>d</u> vanced settings		
	OK Can	cel

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

Advanced settings
802.1X settings 802.11 settings
Specify authentication mode: User or computer authentication Save credentials Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
 Perform immediately after user logon
Maximum delay (seconds):
✓ Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK Cancel

Step 11 Click Close.



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



Step 13 In the **Windows Security** dialog box that appears, enter the <u>user name and password</u> set on the RADIUS server and click **OK**.



--End

Verification

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

7.2 RF Settings

7.2.1 Overview

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

Isolate SSID

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 RF settings

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

RF		
Enable RF	۲	
Country/Region	China	٣
Network Mode	11b/g/n	٣
Channel	Auto	T
Channel Bandwidth	20MHz 40	MHz 💿 20/40MHz
Extension Channel	Auto	٣
Lock Channel		
Isolate SSID	Oisable	Enable
APSD	🔘 Enable	Disable
Client Timeout Interval	5 minutes	•

--End

Parameter	Description
Enable RF	It specifies whether to enable the RF function of the AP.
Country	It specifies the country or region where the AP is used. This parameter helps comply with channel regulations of the country or region.
	It specifies the wireless network mode of the AP.
	Available options include 11b/g, 11b, 11g, and 11b/g/n. This parameter can be set if Lock Channel is not selected.
	• 11b : It indicates that only clients working in the 11b network mode can connect to the AP.
Network Mode	• 11g : It indicates that only clients working in the 11g network mode can connect to the AP.
	• 11b/g : It indicates that only clients working in the 11b or 11g network mode can connect to the AP.
	• 11b/g/n : It indicates that clients working in the 11b, 11g, or 11n network mode can connect to the AP.
Channel	It specifies the operating channel of the AP. This parameter can be set if Channel Lockout is not selected.
	It specifies the bandwidth of the operating channel of the AP. This parameter can be set if Channel Lockout is not selected.
Channel Bandwidth	• 20MHz : It indicates that the AP only uses 20 MHz channel bandwidth.
	• 40MHz : It indicates that the AP only uses 40 MHz channel bandwidth.
	• 20/40MHz: It indicates that the AP automatically adjusts its channel bandwidth to 20

Parameter	Description
	MHz or 40 MHz according to the ambient environment. This option is effective only for 802.11b/g/n mixed network mode.
Extension Channel	It specifies an additional channel used to increase the channel bandwidth if the AP works in the 802.11b/g/n mixed network mode and the channel bandwidth option 40MHz or 20/40MHz is selected.
Lock Channel	It is used to lock the selected channel. After a channel is locked, parameters of the channel cannot be changed, including Country , Network Mode , Channel , Channel Bandwidth , and Extension Channel .
	It specifies whether to isolate the wireless clients connected to the AP with different SSIDs.
Isolate SSID	• 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.
Client Timeout Interval	It is used to set the timeout interval 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 know wireless networks information nearby, including SSID, MAC address, channel and wireless signal strength.

7.3.2 Checking the usage of channels

Step 1 Choose **Wireless** > **Channel Scan**.

Step 2 Click Scan.

Channel Scan		
	Scan	Help

--End

Wait for a moment. The following table shows the scanning result.

Chanr	hannel Scan								
			-						
		Disable Scan					Help		
ID	SSID	MAC Address	Network Mode	Channel	Channel Bandwidth	Security Mode	Signal Strength		
1	Tenda_1	50:2b:73:09:94:51	bgn	10	20	wpa2/aes	0dBm		
2	Tenda_826021	c8:3a:35:4c:cb:71	bgn	2	20	wpa&wpa2/aes	-34dBm		
3	Tenda_FFBF30	50:2b:73:ff:bf:31	bgn	5	20	wpa&wpa2/aes&	-36dBm		
4	default	c8:3a:35:4e:84:d0	bgn	1	20	none	-36dBm		
5	Tenda_826022	c8:3a:35:36:6f:c1	bgn	3	40	wpa&wpa2/aes	-36dBm		
6	Tenda_WiFi	c8:3a:35:07:b3:b1	bgn	4	20	none	-38dBm		
7	Tenda_826020	50:2b:73:82:60:21	bgn	1	20	wpa2/aes	-38dBm		
8	Tenda_50F080	c8:3a:35:e6:49:b1	bgn	13	20	wpa&wpa2/aes	-38dBm		
9	Tenda_D70CA0	50:2b:73:f0:39:d1	bgn	6	20	wpa2/aes	-40dBm		

7.4 WMM Setup

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.



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:

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

	WMM	○Disable ●Enable			Save
WMM	Optimization Mode	Optimized For Throughput	(Concurrent Users <=10)		Resto
		Optimized For Capacity(Co	oncurrent Users >=10)		
		Custom			Help
	No ACK	•			
ED	CA AP Parameters				
	CWmin	CWmax	AIFSN	TXOP Limit(usec)]
AC_BE	7	63	1	4096	
AC_BK	15	1023	7	0	
AC_VI	7	15	1	6016	
C_VO	3	7	1	3264	
EDC	A STA Parameters				_
	CWmin	CWmax	AIFSN	TXOP Limit(usec)]
AC_BE	31	255	2	3200	
AC_BK	15	1023	7	0	
					1

Parameter	Description
WMM	 Enable: It is used to enable the WMM function. Disable: It is used to disable the WMM function.
WMM Optimization Mode	 It specifies the WMM optimization modes supported by the AP: Optimized For Throughput(Concurrent Users <=10): If 10 or less clients are connected to the AP, you are recommended to select this mode to increase client throughput. Optimized For Capacity(Concurrent Users >=10): 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	 If the check box is selected, the No ACK policy is adopted. If the check box is deselected, the Normal ACK policy is adopted.

Parameter	Description
EDCA Parameters	For details, refer to section 7.5.1 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.

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

Advanced		
		_
Beacon Interval	100 ms (Range: 100 - 999; Default: 100) Save	
Fragment Threshold	2346 (Range: 256 - 2346; Default: 2346) Restor	е
RTS Threshold	2347 (Range: 1 - 2347; Default: 2347)	
DTIM Interval	1 (Range: 1 - 255; Default: 1)	
Min. RSSI Threshold	Enable Isable	
Interference Mitigation	2 (Range: 0 - 3; Default: 2)	
Transmit Power	20 • dBm (Range: 8 - 20; Default: 20)	
Lock Power		
Preamble	Long Preamble Short Preamble	

--End

Parameter	Description
Beacon Interval	It specifies the interval for transmitting the Beacon frame. 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.

Parameter	Description
	It specifies the threshold of a fragment. The unit is byte.
	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.
Fragment Threshold	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.
	In an environment without interference, you can increase the threshold to reduce the number of acknowledgement times, so as to increase the frame throughput.
	It specifies the frame length threshold for triggering the RTS/CTS mechanism.
	If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. The unit is byte.
RTS Threshold	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.
	The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
	It specifies the interval for transmitting the Delivery Traffic Indication Message (DTIM) frame. The unit is Beacon.
DTIM Interval	A countdown starts from this value. The AP transmits broadcast and multicast frames in its cache only when the countdown reaches zero.
	For example, if DTIM Interval is set to 1 , the AP transmits all cached frames after each beacon frame is transmitted.
Min. RSSI Threshold	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.
	If there are multiple APs, an appropriate value of this parameter ensures that wireless clients connect to the APs with strong signals.
	Interference mitigation mode. The default is 2.
	• 0: Disable all interference mitigation.
Interference Mitigation	 1: Enable interference mitigation from the same frequency band, like interference from microwave oven, smartphone, or Bluetooth device.
	• 2: Compulsively enable radio waves interference mitigation.
	• 3: Automatically enable radio waves interference mitigation.
Transmit Power	It specifies the transmit power of the AP. Higher transmitted power contributes to wider wireless coverage. But reducing the transmitted power properly can improve the security of your wireless network.

Parameter	Description
Lock Power	It specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.
Preamble	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.
rieamble	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.

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.
- **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

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

₽_{TIP}

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.

Step 5 Click Save.

Ac	cess Co	ontrol				
۲ t	'ou can sp he AP.	ecify MAC address filter r	ules to allow or disallow w	ireless devices to connec	t to the wireless networks of	Save
		SSID	Tenda_888888	• Wi	reless client list	Restore
<i></i>		MAC Filter Mode	Allow	•		Help
	ID	MAC Address	IP	Connection Uptime	Add to List	
	1	1C:5C:F2:B4:40:08	192.168.0.133	00:00:12	Add	
: [[i "``\
MAC Address Operation						
		12 : 12			Add	

Wireless access control list

--End
Parameter description

Parameter	Description
SSID	It specifies the SSID that requires wireless client access control.
	It specifies the mode for filtering MAC addresses.Disable: It indicates that access control is disabled.
MAC Filter Mode	• 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:

- **Step 1** Choose **Wireless** > **Access Control**.
- **Step 2** Select **Home** from the **SSID** drop-down list box.
- **Step 3** Select **Allow** from the **MAC Filter Mode** drop-down list box.
- Step 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.
- **Step 5** Click **Save**.

The following figure shows the configuration.

Access Co	ontrol				
You can sp the AP.	ecify MAC address filter ru	les to allow or disallow wi	reless devices to conne	ect to the wireless networks of	Save
	SSID	Home	•		Restore
	MAC Filter Mode	Allow	T		Help
ID	MAC Address	IP	Connection Uptime	Add to List	
	No client connected.				
	MAC Address Operation				
	C8 : 3A : 35 : 00 : 03 Add				
1	C8:3A:	35:00:00:01	🕑 Enable	Delete	
2	C8:3A:	35:00:00:02	🖉 Enable	Delete	
3	C8:3A:	35:00:00:03	🗷 Enable	Delete	

Verification

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

7.7 QVLAN Settings

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

Step 1 Choose **Wireless** > **QVLAN Setup**.

Step 2 Change the parameters as required. Generally, you only need to change the **Enable**, and VLAN ID settings.

Step 3 Click **Save**.

QVLAN Setup		
★ Enable		Save
PVID	1	Save
Management VLAN	1	Restore
* 2.4G SSID	VLAN ID (1~4094)	Help
Home	1000	

--End

Parameter description

Parameter	Description
Enable	It specifies whether to enable the QVLAN function of the AP. By default, it is disabled.
PVID	It specifies the ID of the default native VLAN of the trunk port of the AP. The default value is 1 .
Management VLAN	It specifies the ID of the AP management VLAN. The default value is 1 . After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
2.4G SSID	It specifies the currently enabled 2.4 GHz SSIDs of the AP.
VLAN ID	It specifies VLAN IDs corresponding to SSIDs. The default value is 1000 . After the QVLAN function is enabled, the wireless interfaces 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 Proces	Method to Process	
	Tagged Data	Untagged Data	Transmitted 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 internal server.
- Managers of the hotel are connected to VLAN 4 and can access the internet and the internal server.

Assumption

The AP enables wireless networks and configures the following SSIDs.

- SSID of the wireless network for guests: internet
- SSID of the wireless network for employees: oa
- SSID of the wireless network for hotel managers: VIP

Network Topology



Configuration procedure:

Configure the AP

- **Step 1** Log in to the web UI of the AP and choose **Wireless** > **QVLAN Setup**.
- **Step 2** Select the **Enable** check box.
- **Step 3** Change the **VLAN ID** of the SSID **internet** to **2**, the **VLAN ID** of the SSID **oa** to **3**, and the **VLAN ID** of the SSID **VIP** to **4**.

Step 4 Click Save.

✓ ★	Save
1	Save
1	Restore
VLAN ID (1~4094)	Help
2 \star	
4 🗙	
3 🛪	
	<pre> * 1 1 1 1 VLAN ID (1~4094) 2 * 4 * 3 * </pre>

--End

Wait for the automatic reboot of the AP.

Configure the switch

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

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

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

Configure the router and the internal server

To ensure that wireless devices connected to the AP can access the internet, the router and internal server are required to support the QVLAN function. Refer to the following details:

For the router:

Port Connected To	Accessible VLAN ID	Port Type	PVID		
Switch	2, 4	Trunk	1		
For the internal server:					
Port Connected To	Accessible VLAN ID	Port Type	PVID		
Switch	3, 4	Trunk	1		

For details of configuration procedure, refer to the user guide of the router and the internal server.

--End

Verification

Wireless clients connected to the **internet** wireless network can access only the internet, the wireless clients connected to the **oa** wireless network can access only the internal server, and wireless clients connected to **VIP** wireless network can both access the internet and the internal server.



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 calling 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

- **Step 1** Choose **SNMP** and set **SNMP Agent** to **Enable**.
- **Step 2** Set related SNMP parameters.

Step 3 Click Save.

<u>SNMP</u>		
You can configure SNMP V1 o SNMP Agent	n SNMP V2C settings here.	Save
Administrator	Administrator	Restore
AP Name	i9V2.0	Help
Location	ShenZhen]
Read Community	public]
Read/Write Community	private	

--End

Parameter description

Parameter	Description
	It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled.
SNMP Agent	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.
Administrator	It specifies the name of the administrator of the AP. The default name is Administrator . You can change the location as required.
	It specifies the name of the AP. The default device name is in the format of Model + Hardware version number.
AP Name	
	It is recommended that you change the AP name so that you can easily identify the AP when managing the AP using SNMP.
Location	It specifies the location where the AP is used. You can change the location as required.
Read Community	It specifies the read password shared between SNMP managers and this SNMP agent. The default password is public .
icua community	The SNMP agent function of the AP allows an SNMP manager to use the password to read variables in the MIB of the AP.
Read/Write Community	It specifies the read/write password shared between SNMP managers and this SNMP agent. The default password is private .
Kead/ Write Community	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.

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**.

- **Step 1** Log in to the web UI of the AP and choose **SNMP**.
- **Step 2** Set **SNMP Agent** to **Enable**.
- **Step 3** Set the SNMP parameters.
- Step 4 Click Save.

<u>SNMP</u>		
You can configure SNMP V1	or SNMP V2C settings here.	Save
SNMP Agent	 Disable Enable 	
Administrator	Tom	Restore
AP Name	i9V2.0	Help
Location	Room	
Read Community	Tom	
Read/Write Community	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.



9.1 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.

Configuration procedure:

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

Firmware Upgrade Administrate	or:admin	
You can upgrade the AP firmware for more functionalities or better performance.		
Select a Firmware File: Choose File No file chosen Upgrade		
Current Firmware Version: V1.0.0.6(1020); Release Date: 2017-11-28		
Note: Do not power off the AP when an upgrade is in process. Otherwise, the AP may be damaged. When an upgrade is complete, the AP reboots automatically. An upgrade takes about 90 seconds. Please wait.		

--End

Wait until the progress bar 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.

9.2 Time & Day

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

9.2.1 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** > **Date & Time**.

System Time	Login Timeout	
You can configu	re the system time of the AP here.	Save
Note: The system	time is lost when the AP is turned off. It will be synchronized with the GMT time automatically when	
the AP is turned	on and connected to the internet again.	Restore
Synchronize w	ith internet time Sync Interval: 30 minutes 🔹	
Time Zone: (0	GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei	Help
Note: The system	is automatically synchronized with the GMT time only after the AP is connected to the Internet.	
Enter Date and T	ime:	
2018 Y	10 M 12 D 13 h 44 m 39 s Synchronize with PC Time	

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.

Synchronizing 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:

- **Step 1** Choose **Tools > Date & Time > System Time**.
- **Step 2** Select the **Synchronize with internet time** check box.
- **Step 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.
- **Step 4** Set **Time Zone** to your time zone.
- **Step 5** Click **Save**.

System Tin	ne Login Timeout				
You can conf Note: The sys the AP is turn	igure the system time of the AP here. stem time is lost when the AP is turned off. It wil ned on and connected to the internet again.	ll be synch	ronized with the GMT time automa	atically when	Save
✓Synchroniz	re with internet time Sync 1	Interval:	30 minutes	•	
Time Zone:	(GMT+08:00) Beijing, Chongqing, Hong Kong	, Urumqi, 1	Taipei	•	Неір
Note: The sys	stem is automatically synchronized with the GMT	time only	after the AP is connected to the Ir	nternet.	
Enter Date an	id Time:				
2018	Y 10 M 12 D 13 h 44 m 39 s S	synchronize	e with PC Time		

--End

Manually setting the system time

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.

Configuration procedure:

- **Step 1** Choose **Tools > Date & Time > System Time**.
- **Step 2** Deselect **Sync with internet time servers**.
- **Step 3** 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.
- Step 4 Click Save.

System Tin	ne Login Timeout	
You can conf	igure the system time of the AP here.	Save
Note: The sys	stem time is lost when the AP is turned off. It will be synchronized with the GMT time automatically when	
the AP is turr	ed on and connected to the internet again.	Restore
Synchroniz	e with internet time Sync Interval: 30 minutes 🔻	
Time Zone:	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei	Help
Note: The sys	stem is automatically synchronized with the GMT time only after the AP is connected to the Internet.	
Enter Date ar	id Time:	
2018	Y 10 M 12 D 13 h 44 m 39 s Synchronize with PC Time	

9.2.2 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:

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

Step 3 Click Save.

System Time Login Timeout	
Login Timeout: 5 minute (Range: 1 - 60)	Save
	Restore
	Help

9.3 Logs

9.3.1 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**.

View Log	js Log Settings			
		Ту	pe of Logs to Display: All 🔻	Refresh
ID	Time	Туре	Log Content	Clear
37	2018-10-12 13:49:52	system	Sync time success!	
36	2018-10-12 13:40:34	system	web 192.168.0.104 login	
35	2018-10-12 13:15:44	system	Sync time success!	
34	2018-10-12 12:45:52	system	Sync time success!	
33	2018-10-12 12:28:18	system	web 192.168.0.104 login time expired	
32	2018-10-12 12:13:52	system	Sync time success!	
31	2018-10-12 11:56:48	system	2.4GHz WiFi up	
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** > **Date & Time** > **System Time**.

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

- 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.

9.3.2 Log settings

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

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

View Log	js Log Settin	igs				
Number o	f Logs Displayed	150	(Range: 100	- 300; Default: 15())	Save
🗌 Enabl	e Log Server Functio	on				Restore
ID	Log Server I	P Address	Log Server Port	Enable	Operation	
					Add	Help

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.

Configuration procedure:

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

View Lo	gs Log Settin	<u>gs</u>				
* Number o	f Logs Displayed	150	(Range: 100	- 300; Default: 150))	Save
🗌 Enab	le Log Server Functio	in				Restore
ID	Log Server I	P Address	Log Server Port	Enable	Operation	
	·					Help
					Add	

Configuring log server settings

After a log server is specified, 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:

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

Step 2 Click Add.

iew Log	s Log Settings				
Number of	Logs Displayed 150	(Range: 100	- 300; Default: 150))	Save
Enable	Log Server Function				Restore
ID	Log Server IP Address	Log Server Port	Enable	Operation	
				Add	Help

Step 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 this log server rule.

Step 4 Click Save.

View Logs Log Settings		
Log Server IP Address		Save
Log Server Port	514	Restore
Enable		Help

- **Step 5** Select **Enable Log Server function**.
- **Step 6** Click **Save**.

The following figure shows the configuration.

View Lo	gs Log Settin	gs				
Number (of Logs Displayed	150	(Range: 100 -	300; Default: 150)	Save
🕑 Enab	le Log Server Functio	on				Restore
ID	Log Server I	P Address	Log Server Port	Enable	Operation	
1	192.168	.0.88	514	Enable	Change Delete	Help
					Add	;]

Procedure for changing log server settings

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

--End

Procedure for deleting log server settings

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

9.4 Configuration

9.4.1 Backup & Restore

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

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

Backup & Restore	Restore Factory Settings	
You can back up the curr	ent AP configuration or restore an original AP configuratio	n here.
Back Up Configuration	Backup	
Restore Configuration	Choose File No file chosen	Restore



Restoring a Configuration

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

--End

9.4.2 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**.

- 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

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

Backup & Restore Restore Factory Settings	
Clicking the Reset button restores the factory settings of the AP.	Help
Restore Factory Settings	

--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.

Configuration procedure:

Step 1 When the AP is working properly, hold down the reset button for 8 seconds.



Step 2 Wait about 1 minute.

9.5 Account

To access page for changing user names and passwords, choose **Tools > Account**.

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

Account				
You can change your logir Note: Only 1 to 32 letters,	n user name and password he digits, and underscores are a	ere. allowed in a user name	or password.	Save
Account Type	User Name	Enable	Operation	Restore
Administrator	admin	I.	Change	Help
User	user	I.	Delete Change	

Parameter description

Parameter	Description
Account Type	• Administrator: 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.
	It specifies the user name of an account.
User Name	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 .
	It specifies whether an account is enabled.
Enable	 The administrator account is always enabled.
	 The user account is enabled by default and can be disabled.
	Change : This button is used to change the user name and password of the account corresponding to the button.
Operation	Delete: This button is used to delete the user account.
	After changing or deleting an account, click Save.

9.6 Diagnostics Tool

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

Configuration procedure:

The link to <u>www.google.com</u> is used as an example.

- **Step 1** Choose **Tools** > **Diagnostics**.
- **Step 2** Enter the IP address or domain name to be pinged in the **Input** text box. In this example, enter **www.google.com**.

Step 3 Click ping.

Diagno	stics Tool		
Enter ar	IP address to be pinged (ex	ample: ping 192.168.0.254).	
Input:	ping	ping	

--End

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

Diagnostics Tool
Enter an IP address to be pinged (example: ping 192.168.0.254).
Input: ping www.google.com ping
PING www.google.com (31.13.72.54): 56 data bytes
www.google.com ping statistics
3 packets transmitted, 0 packets received, 100% packet loss

9.7 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.

9.7.1 Manual Reboot

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

Configuration procedure:

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

Manual Reboot	Automatic Reboot
You can click the Re	eboot button here to reboot the AP.
Fou can check the he	Reboot

--End

9.7.2 Automatic Reboot

Automatic Reboot allows you to reboot the AP at your specified time to avoid unstable WLAN performance due to long- time running. The AP supports the following two ways of automatic reboot.

Rebooting the AP at an interval

Configuration procedure:

- **Step 1** Choose **Tools > Device Reboot** and click the **Automatic Reboot** tab.
- **Step 2** Select the **Enable Auto Reboot** check box.
- **Step 3** Set **Reboot Mode** to **At intervals**.
- **Step 4** Set **Interval** to a value in minutes, such as **1440**.
- **Step 5** Click **Save**.

Manual Reboot Automa	tic Reboot	
Enable Auto Reboot		Save
Reboot Mode	At intervals	Restore
Interval	1440 minute (Range: 10 - 7200)	Help

--End

Rebooting the AP at specified time

Configuration procedure:

- **Step 1** Choose **Tools > Device Reboot** and click the **Automatic Reboot** tab.
- **Step 2** Select the **Enable Auto Reboot** check box.
- **Step 3** Set **Reboot Mode** to **At specified time**.
- **Step 4** Select the day or days when the AP reboots.
- **Step 5** Set the time when the AP reboots, such as **23:59**.

Step 6 Click **Save**.

Manual Reboot Automa	ntic Reboot	
Enable Auto Reboot	\checkmark	Save
Reboot Mode	At specified time	Restore
Date	🗌 Every day 🕜 Mon. 🕜 Tue. 🕜 Wed. 🕜 Thur. 🖉 Fri. 🗌 Sat. 🗌 Sun.	Help
Time	23:59 Example: 3:00	

9.8 LED Control

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

Procedure for turning off the LED indicator:

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

LED Control		
		Help
	Turn Off All Indicators	

--End

Procedure for turning on the LED indicator:

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

Appendixes

A.1 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, connect one of the APs to your network and change the IP address of the AP. Repeat this procedure to change the IP addresses of the other APs.
- 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 you have manually changed the IP address of the AP, change the IP address of your computer to another IP address that belongs to the same network segment as the new IP address of the AP and log in again using the new IP address of the AP.
- 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. Can I log in to the web UI of the AP to configure the AP after using an AC controller to manage the AP?

A3. Yes. You are recommended to change the user name and password of the administrator account (see <u>9.5 Account</u>) if you use an AC to manage the AP. This improves network security.

For more technical assistance, visit our website at <u>http://www.tendacn.com</u> or send your question to <u>support@tenda.cn</u>. We will help you resolve your problem as soon as possible.

A.2 Setting the IP Address of Your Computer

Example: Windows 7

- **Step 1** Choose **Start > Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Change adapter settings**.
- **Step 2** Right-click **Local Area Connection** and choose **Properties**. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

📮 Local Area Connection Properties 📃 💌		
Networking Sharing		
Connect using:		
Intel(R) 82583V Gigabit Network Connection		
Configure This connection uses the following items:		
 Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 4 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder 		
Install Uninstall Properties		
Description		
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.		
OK Cancel		

Step 3 Select Use the following IP address. Set IP address to an IP address that is different from the IP address of the LAN port of the AP but belongs to the same network segment as the IP address of the LAN port of the AP. Set Subnet mask to 255.255.255.0. Click OK.

Internet Protocol Version 4 (TCP/IPv4) Properties			
General			
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.			
🔘 Obtain an IP address automatical	У		
• Use the following IP address:			
IP address:	192.168.0.10		
Subnet mask:	255 . 255 . 255 . 0		
Default gateway:	· · ·		
Obtain DNS server address autom	natically		
• Use the following DNS server add	resses:		
Preferred DNS server:			
Alternate DNS server:			
Validate settings upon exit	Ad <u>v</u> anced		
	OK Cancel		

The Local Area Connection Properties dialog box appears.

Step 4 Click OK.

A.3 Default Parameter Settings

The following table lists the factory settings of the AP.

Parameter			Default Value
Login	IP address		192.168.0.254
	User Name/Password	Administrator	admin/admin
	User Name/Fassword	User	user/user
Quick Setup	Working Mode		AP Mode
	IP Address Type		Static
	IP Address (manageme	ent IP address)	192.168.0.254
	Subnet Mask		255.255.255.0
LAN Setup	Gateway		192.168.0.1
	Primary DNS Server		8.8.8.8
	Secondary DNS Server		8.8.4.4
	Device Name		Model + Hardware version number, such as i9V2.0
	DHCP Server		Disable
	Start IP		192.168.0.100
	End IP		192.168.0.200
DHCP Server	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
Wireless Basic	SSID		Supports 4 SSIDs. SSID is Tenda_XXXXXX, where XXXXXX indicates the last 6 characters in the MAC address specified on the label on the external surface of the AP - +3 The primary SSID is enabled, and others are disabled.
	Broadcast SSID		Enable
	Isolate Client		Disable

Parameter		Default Value
	WMF	Disable
	Max. Number of Clients	32
	Chinese SSID Encoding	UTF-8
	Security Mode	None
	Wireless network	Enable
	Network Mode	11b/g/n
	Channel	Auto
	Channel Bandwidth	20/40 MHz
RF	Extension Channel	Auto
	Lock Channel	Enable
	Isolate SSID	Disable
	APSD	Disable
	Client Timeout Interval	5 minutes
	Beacon Interval	100 ms
	Fragment Threshold	2346
	RTS Threshold	2347
	DTIM Interval	1
Wireless Advanced	Min. RSSI Threshold	Disable
	Interference mitigation	2
	Transmit Power	20 dBm
	Lock Power	Enable
	Preamble	Long Preamble
	WMM function	Enable
	WMM Optimization Mode	Optimized For Capacity (Concurrent Users >=10)
Wireless Access Control		Disable
	QVLAN function	Disable
QVLAN	PVID	1
	Management VLAN	1

Parameter			Default Value
	2.4 GHz SSID VLAN ID		1000
SNMP	SNMP Agent		Disable
	SNMP Parameters	Administrator Name	Administrator
		AP Name	Model + Hardware version number, such as i9V2.0
		Location	ShenZhen
		Read Community	public
		Read/Write Community	private
Tools	System Time	Synchronize with internet Time	Enable
		Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei
	Login Timeout		5 minutes
	Number of Logs Displayed		150
	Automatic Reboot		Disable
	LED Control		LED indicators turn on