airlive®

User's Manual

Wi-Fi 5Ghz N300

Outdoor CPE

► AirMax5x II

Contents

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing AirLive AirMax5x II Wireless AP. Please verify the contents inside the package box.

Package Contents of AirMax5X II			
AirMax 5X II	Quick Guide	Ethernet Cable	Mounting Strap
			

Note

If there is any item missing or damaged, please contact the seller immediately.

1.2 Product Description

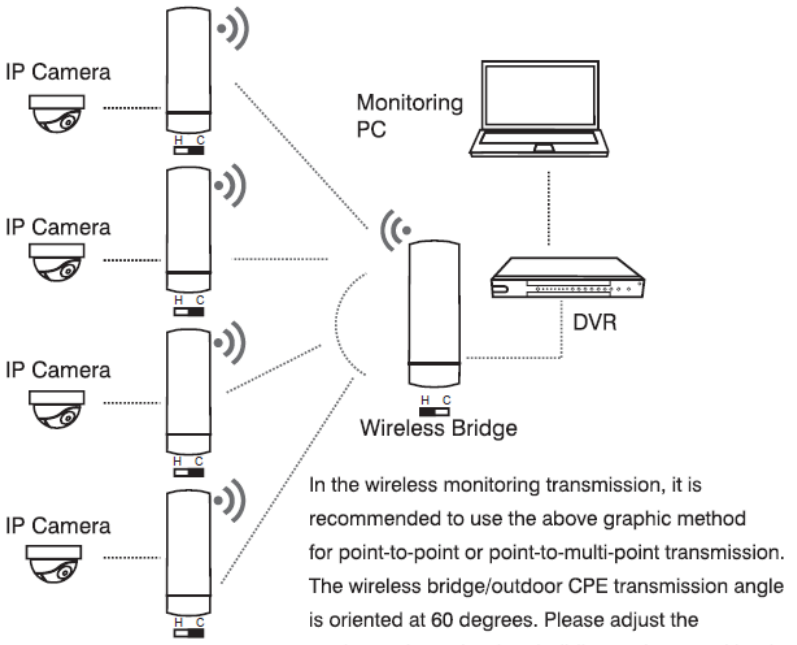
Flexible and Reliable Outdoor Characteristics

With the passive PoE design, the AirMax5X II(outdoor wireless CPE) can be easily installed in the areas where power outlets are not available. The outdoor wireless CPE is definitely suitable for wireless IP surveillance, and br idge link of building to building and backbone of public service. Additionally, the **self-healing** capability keeps connection alive all the time. With the **IP65-rated** outdoor enclosure, the outdoor wireless CPE can perform normally under rigorous weather conditions, meaning it can be installed in any harsh, outdoor environments

Designed for Various Requirements

The outdoor wireless CPE is specially designed for long-distance outdoor surveillance and wireless backhaul solutions that are capable of establishing stable bridge connection through the embedded antenna. To provide maximum performance, the outdoor wireless CPE can implement up to AP/Repeater operation modes where a multitude of applications in communities, warehouses, campuses, harbors, etc. can be made.

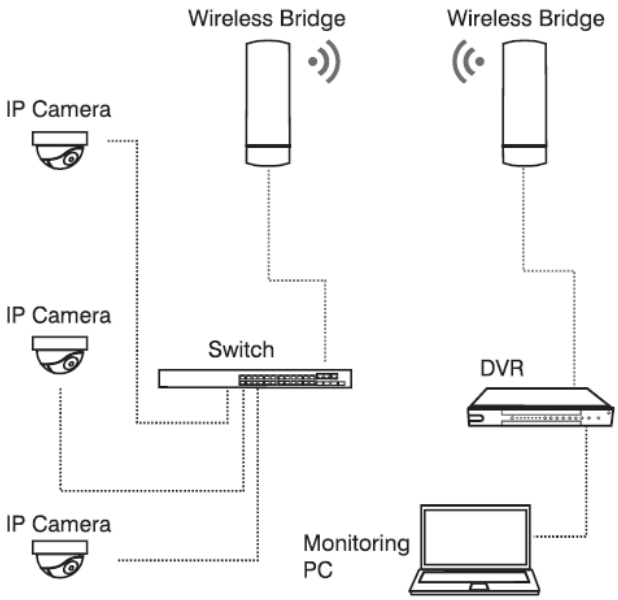
Point to multiple point



In the wireless monitoring transmission, it is recommended to use the above graphic method for point-to-point or point-to-multi-point transmission. The wireless bridge/outdoor CPE transmission angle is oriented at 60 degrees. Please adjust the equipment's angle when building point-to-multi-point transmission.

IP Camera ---- Wireless Bridge Wireless Bridge ---- DVR ---- Monitoring PC

Point to Point



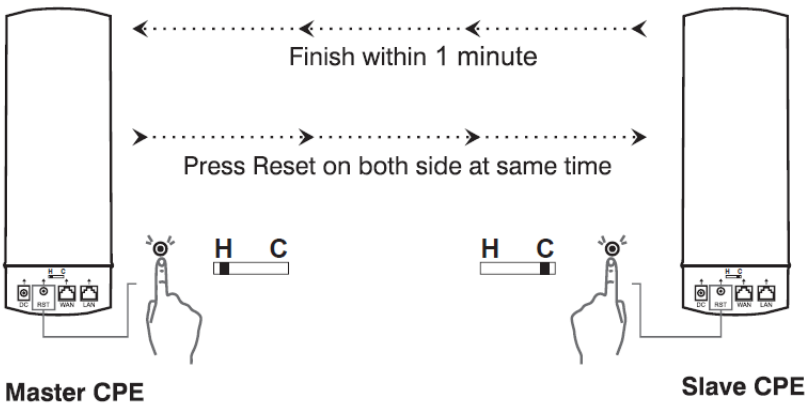
IP Camera --Switch --Wireless Bridge Wireless Bridge--- DVR ---Monitoring PC

Multiple SSIDs with VLAN Tagging

The outdoor wireless CPE supports WPA/WPA2, and the 802.1X RADIUS authentication to secure the wireless connection. Besides, the supported IEEE 802.1Q VLAN allows multiple VLAN tags to be mapped to multiple SSIDs to distinguish the wireless access. This makes it possible for the outdoor wireless CPE to work with managed Ethernet switches to have VLANs assigned to a different access level and authority.

3 Simple Steps to Set Up Point to Point/Point to Multi-Point

Without needing to enter the Web interface for configuration, the outdoor wireless CPE needs three simplesteps to establish the PtP/PtMP connection without any difficulty. By just clicking the **Pair** button on the AirMax5X II and within 2 minutes, you can connect two AirMax5X IIs without complicated configuration.



Optimized Efficiency in AP Management

The brand-new GUI configuration wizard helps the system administrator easily set up the outdoor wireless CPE step by step. Besides, the built-in Wi-Fi analyzer provides real-time channel utilization to prevent channel overlapping to assure greater performance. With the automatic transmission power mechanism, distance control and scheduling reboot setting, the outdoor wireless CPE is easier for the administrator to deploy and manage without on-site maintenance. Moreover, you can simply use AirLive AP Controller, to deliver wireless profiles to multiple APs simultaneously, thus making the central management simple.

1.3 Product Features

- **Industrial Compliant Wireless LAN and LAN**
  - Compliant with the IEEE 802.11b/g/n and IEEE 802.11a/n wireless technology
  - 2T2R architecture with data rate of up to 300Mbps
  - Equipped with two 10/100Mbps RJ45 ports with auto MDI/MDI-X supported
- **Fixed Network Broadband Router**
  - Supported WAN connection types: DHCP, Static IP, PPPoE
  - Supports Port Forwarding and DMZ for various networking applications
  - Supports DHCP server
- **RF Interface Characteristics**
  - Built-in 14dBi dual-polarization antenna (AirMax5X II)
  - Built-in 10dBi dual-polarization antenna (AirMax2X II)
- **Outdoor Environmental Characteristics**
  - IP65 rating
  - Passive PoE 48VDC inject
  - Operating temperature: -20~70 degrees C
- **Multiple Operation Modes and Wireless Features**
  - Multiple operation modes: AP, Repeater
  - WMM (Wi-Fi multimedia) provides higher priority to multimedia transmitting over wireless
  - Coverage threshold to limit the weak signal of clients occupying session
  - Real-time Wi-Fi channel analysis chart and client limit control for better performance
- **Secure Network Connection**
  - Full encryption supported: WPA/WPA2, WPA-PSK/WPA2-PSK and 802.1X RADIUS authentication
  - Supports 802.1Q VLAN and SSID-to-VLAN mapping
  - Supports IP/Port/MAC address/URL filtering, DoS, SPI Firewall
  - Supports DMZ and Port Forwarding
  - Bandwidth control per IP address to increase network stability
- **Easy Installation and Management**
  - 3 simple steps to establish WDS connection easily
  - Supports AirLive AP Controllers in AP mode
  - Self-healing mechanism through system auto reboot setting
  - System status monitoring through remote Syslog Server

1.4 Product Specifications

Model Name	AirMax2 II	AirMax5X II
Description	AirMax5X II: 5.8GHz 802.11n 300Mbps Outdoor Wireless CPE AirMax2N: 2.4GHz 802.11n 300Mbps Outdoor Wireless CPE	
Hardware Features		
Interfaces	Wireless IEEE802.11 a/n, 2T2R	Wireless IEEE 802.11a/b/n, 2T2R
	PoE: 1 x 10/100BASE-TX, auto-MDI/MDIX, Passive PoE PD LAN: 1x 10/100BASE-TX, auto-MDI/MDIX	
Antennas	Built-in 8dBi directional antenna with dual polarization	Built-in 14dBi directional antenna with dual polarization
Button	Reset/Pair button, WiFi Mode Switch	
Dimensions	26.19*8.82*5.82 cm	
Weight	405g	
Power Requirements	48V Passive PoE	
Power Consumption	< 13W	
Wireless Interface Specifications		
Standard	IEEE 802.11b/g/n IEEE 802.11i IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3x flow control	IEEE 802.11a/n IEEE 802.11i IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3x flow control
Media Access Control	CSMA/CA	
Modulation	802.11b/g/n: OFDM (BPSK/ QPSK/ 16QAM/ 64QAM) 802.11b: DSSS (DBPSK/ DQPSK/ CCK)	802.11a/n: OFDM (BPSK/ QPSK/ 16QAM/ 64QAM)
Frequency Band	FCC: 2.412~2.462GHz ETSI: 2.412~2.472GHz	FCC: 5.180~5.240GHz, 5.745~5.825GHz ETSI: 5.180~5.700GHz
Operating Channels	FCC: 1~11 Channels ETSI: 1~13 Channels	FCC: 36, 40, 44, 48, 149, 153, 157, 161, 165 (9 channels) ETSI: 36, 40, 44, 48, 100, 104, 108, 112, 116, 132, 136, 140 (16 channels) **5GHz channel list will very in different countries according to their regulations.**
Max. Transmit Power (dBm)	FCC: up to 20 dBm ETSI: < 20dBm (EIRP)	FCC: up to 26dBm ETSI: < 20dBm (EIRP)

	Network Mode	Data Rate	Receive Sensitivity (dBm)	Network Mode	Data Rate	Receive Sensitivity (dBm)
	802.11b	1Mbps	-95			

		11Mbps	-90			
	802.11g	6Mbps	-90	**802.11a**	6Mbps	-92
		54Mbps	-72		54Mbps	-75
	802.11n HT20	MCS0/MCS 8	-90	**802.11n HT20**	MCS0/MC S8	-91
		MCS7/MCS 15	-72/-68		MCS7/MC S15	-72
	802.11n HT40	MCS0/MCS 8	-90	**802.11n HT40**	MCS0/MC S8	-88
		MCS7/MCS 15	-72/-68		MCS7/MC S15	-70
Environment & Certification						
Operating Temperature	-30 ~ 70 degrees C					
Operating Humidity	5 ~ 95% (non-condensing)					
IP Level	IP65					
ESD Protection	± 8kV air-gap discharge ± 6kV contact discharge					
Surge Protection	± 4kV					
Regulatory	CE, RoHS					
Software						
LAN	Static IP					
	Supports IP-MAC binding					
WAN Type (GW/WISP mode)	■ Static IP ■ Dynamic IP ■ PPPoE					
Wireless Modes	■ Access Point ■ Repeater					
Channel Width	20MHz, 40MHz					
Encryption Type	WPA, WPA-PSK, WPA2, WPA2-PSK, 802.1X					
Wireless Security	Enable/Disable SSID Broadcast					
	Wireless MAC address filtering					
	User Isolation					
Max. SSIDs	4					
Max. Wireless Clients	64 per radio					
Max. WDS Peers	4 (Up to 3 peers)					

Wireless QoS	Supports Wi-Fi Multimedia (WMM)
Wireless Advanced	Auto Channel Selection
	WLAN Partition
	Client Limit Control, Coverage Threshold
	Distance control (Auto Ack Timeout)
	Wi-Fi channel analysis chart
	Fast Roaming
Status Monitoring	Device status, wireless client List
	AirLive Smart Discovery
	DHCP client table
	System Log supports remote syslog server
VLAN	IEEE 802.1Q VLAN (VID: 3~4094)
	SSID-to-VLAN mapping up to 4 SSIDs
Self-healing	Supports auto reboot settings per day/hour
Management	Remote management through WEB/Telnet
	Configuration backup and restore
	Supports UPnP
	Supports IGMP Proxy
	Supports PPTP/L2TP/IPSec VPN Pass-through

Chapter 2. Hardware Installation

2.1 Product Outlook

AirMax5X II/2X II

- **Dimensions**: 87 x 38 x 260mm

Front Side

Figure 2-1 AirMax5X II/2X II Front Side

Rear Side

Figure 2-2 AirMax5X II/2XII Rear Side

Right Side

Figure 2-3 AirMax5X II Right Side

Figure 2-4 AirMax2X II Right Side

LED Definition

LED	State	Meaning
Power	On	The device is powered on
	Off	The device is powered off
WAN Port	On	Port linked
	Blinking	Data is transmitting or receiving data
	Off	No link
LAN Port	On	Port linked
	Blinking	Data is transmitting or receiving data
	Off	No link
WLAN	On	The wireless radio is on
	Blinking	Data is transmitting or receiving over wireless
	Off	The wireless radio is off

Port and Button

It provides a simple interface monitoring the AP. Figure 2-5 shows the hardware interface of the AirMax5X II/2XII.

AirMax5X II/2XII Hardware Interface:

Figure 2-5 AirMax5X II Interface

Hardware Description

Hardware Interface Definition

Object	Description
PoE LAN Port	10/100Mbps RJ45 port, auto MDI/MDI-X
LAN Port	10/100Mbps RJ45 port, auto MDI/MDI-X
PtP Switch	Position "**Master**" to "**Slave**" on the AP.
Reset/Pair Button	Press and hold the **Reset** button on the device for over 15 seconds to return to the factory default setting. Press the "**Reset/Pair**" button on both APs to be connected in 2 minutes. The connection has been successfully established.

Chapter 3. Connecting to the CPE

3.1 System Requirements

- Broadband Internet Access Service (Cable/xDSL/Ethernet connection)
- Passive PoE 48V(supply power to the AirMax5X II/2XII)
- PCs with a working Ethernet adapter and an Ethernet cable with RJ45 connectors
- PCs running Windows 98/ME, NT4.0, 2000/XP, Windows Vista / Win 7, MAC OS 9 or later, Linux, UNIX or other platforms compatible with **TCP/IP** protocols

Note

1. The CPE in the following instructions refers to AirLive AirMax5X II.
2. It is recommended to use Internet Explorer 11, Firefox or Chrome to access the CPE.

3.2 Installing the CPE

Before installing the CPE, make sure your PoE switch is connected to the Internet through the broadband service successfully at this moment. If there is any problem, please contact your local ISP.

Please install the AP according to the following steps. Don't forget to pull out the power plug and k eep your hands dry.

Step 1. Push the latch on the bottom of the Outdoor Wireless CPE to remove the sliding cover.

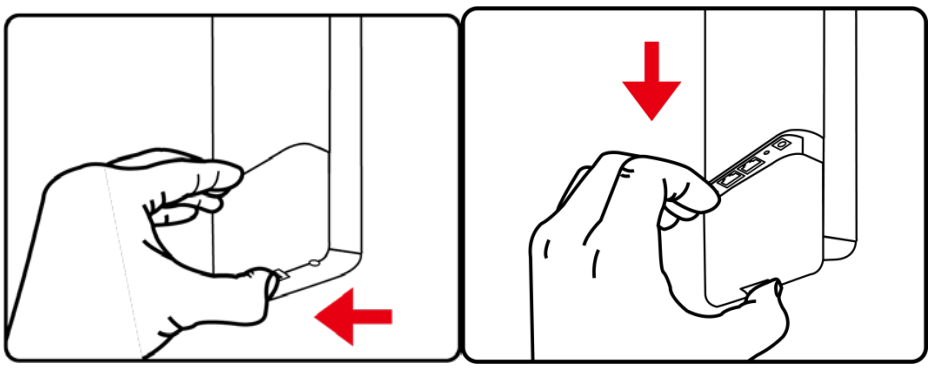


Figure 3-1 Connecting the Antenna

Step 2. Plug the RJ45 Ethernet cable into the PoE port of the Outdoor Wireless CPE. Then, slide back the cover to finish the installation.

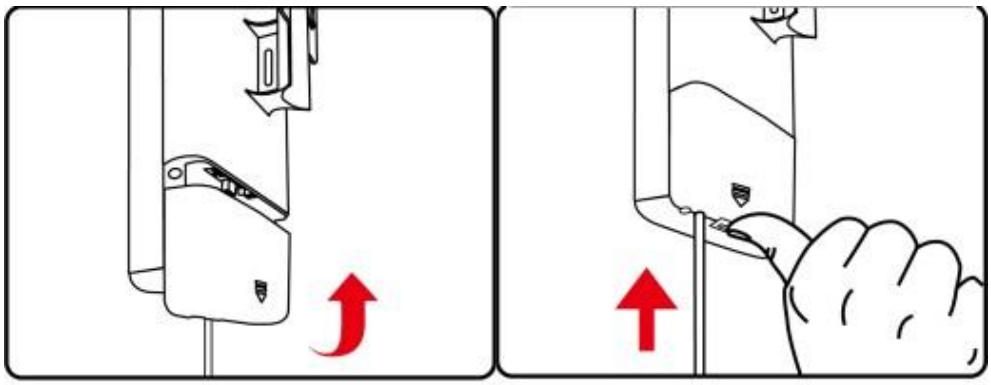


Figure 3-2 Connecting the Ethernet cable

Step 3. Place the mounting strap through the slot on the back of the Outdoor Wireless CPE and then around the pole. Tighten the mounting strap to secure the Outdoor Wireless CPE.

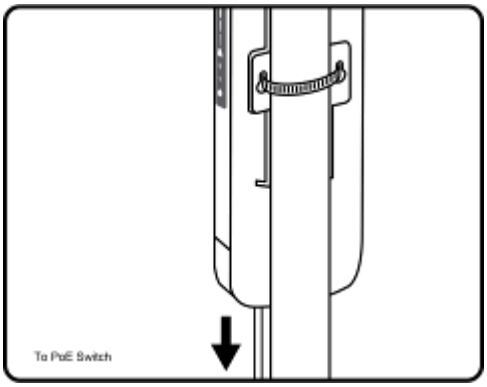


Figure 3-3 Connecting the PoE injector

Chapter 4. Quick Installation Guide

This chapter will show you how to configure the basic functions of your CPE within minutes.

Note

A computer with wired Ethernet connection to the Wireless CPE is required for the first-time configuration.

4.1 Manual Network Setup -- TCP/IP Configuration

The default IP address of the AirMax5X II is **192.168.1.253**. And the default Subnet Mask is 255.255.255.0. These values can be changed as you want. In this guide, we use all the default values for description.

Connect the AirMax5X II with your PC by an Ethernet cable plugging in LAN port on one side and in LAN port of PC on the other side. Please power on the AirMax5X II by PoE switch through the PoE port.

In the following sections, we'll introduce how to install and configure the TCP/IP correctly in **Windows 10**. And the procedures in other operating systems are similar. First, make sure your Ethernet Adapter is working, and refer to the Ethernet adapter manual if needed.

Configuring the IP Address Manually

Summary:

- Set up the TCP/IP Protocol for your PC.
- Configure the network parameters. The IP address is 192.168.1.xxx (If the default IP address of the AirMax5X II is 192.168.1.253, and the DSL router is 192.168.1.254, the "xxx" can be configured to any number from 1 to 252.) and subnet mask is 255.255.255.0.

1 Select **Use the following IP address**, and then configure the IP address of the PC.

2 For example, as the default IP address of the AirMax5X II is 192.168.1.253 and the DSL router is 192.168.1.254, you may choose from 192.168.1.1 to 192.168.1.252.

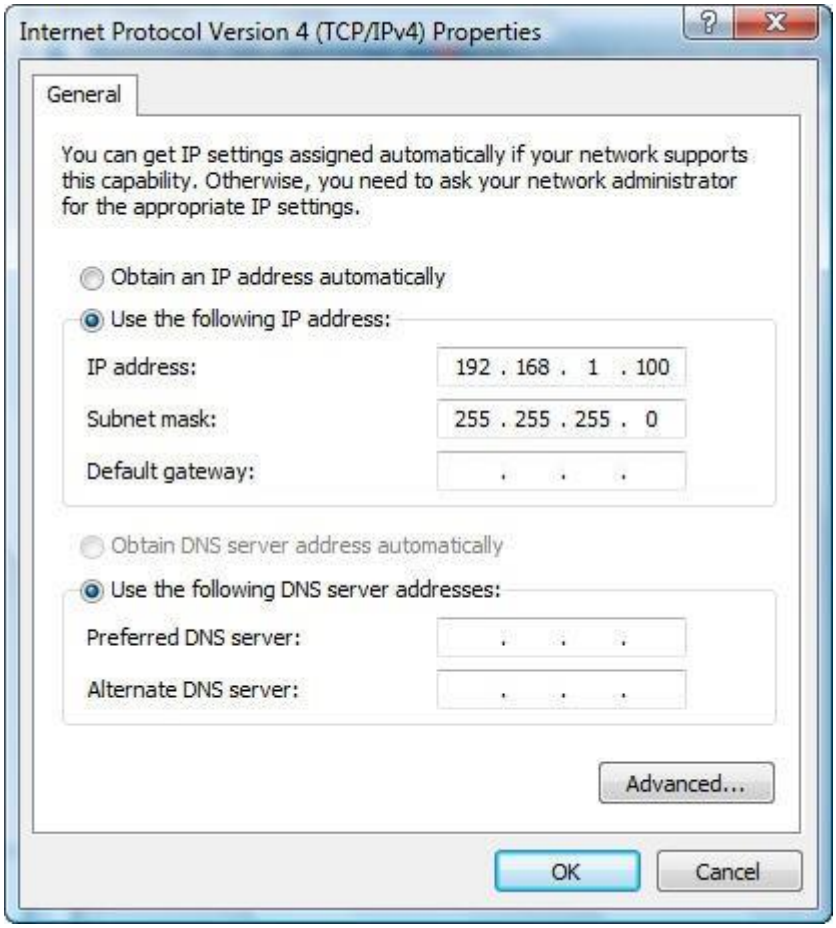


Figure 4-1 TCP/IP Setting

Now click **OK** to save your settings.

Now, you can run the ping command in the **command prompt** to verify the network connection between your PC and the AP. The following example is in **Windows 10** OS. Please follow the steps below:

1. Click on **Start > Run**.
2. Type "**cmd**" in the Search box.

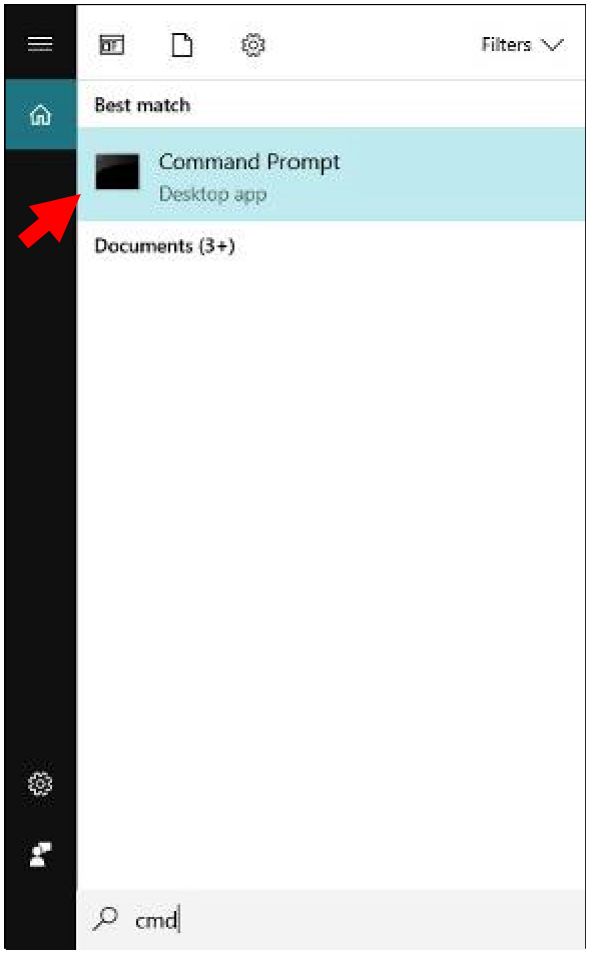


Figure 4-2 Windows Start Menu

3. Open a command prompt, type ping **192.168.1.253** and then press **Enter**.

- If the result displayed is similar to **Figure 4-3**, it means the connection between your PC and the AP has been established well.

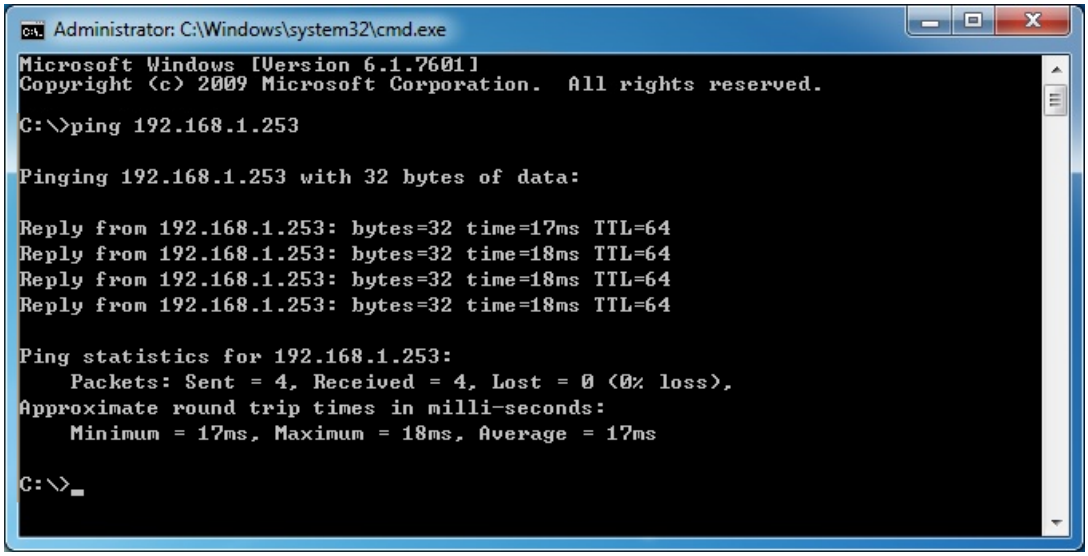


Figure 4-3 Successful Result of Ping Command

- If the result displayed is similar to **Figure 4-4**, it means the connection between your PC and the AP has failed.

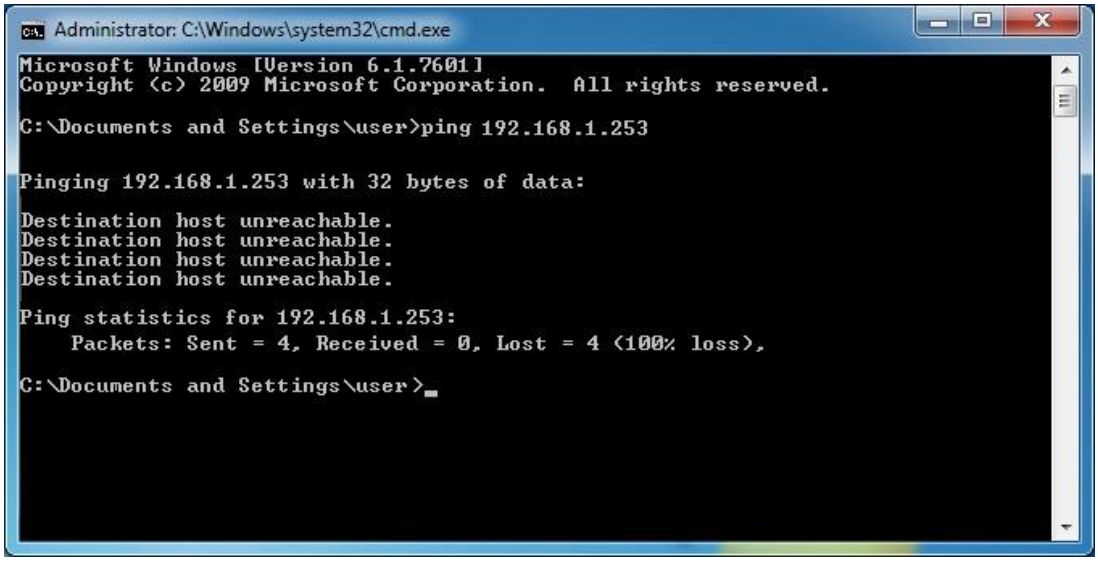


Figure 4-4 Failed Result of Ping Command

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your AP. Some firewall software programs may block a DHCP request on newly installed adapters.

4.2 Starting Setup in the Web UI

It is easy to configure and manage the CPE with the web browser.

Step 1. To access the configuration utility, open a web-browser and enter the default IP address http://192.168.1.253 in the web address field of the browser.

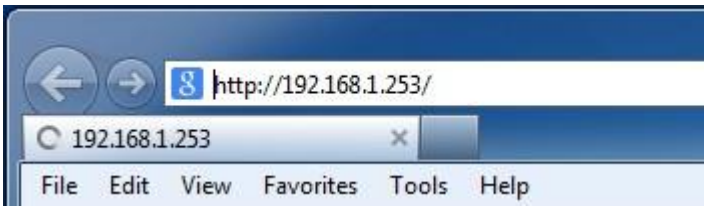


Figure 4-5 Login by Default IP Address

After a moment, a login window will appear. Enter **admin** for the password in lower case letters. Then click **LOGIN** or press the **Enter** key.

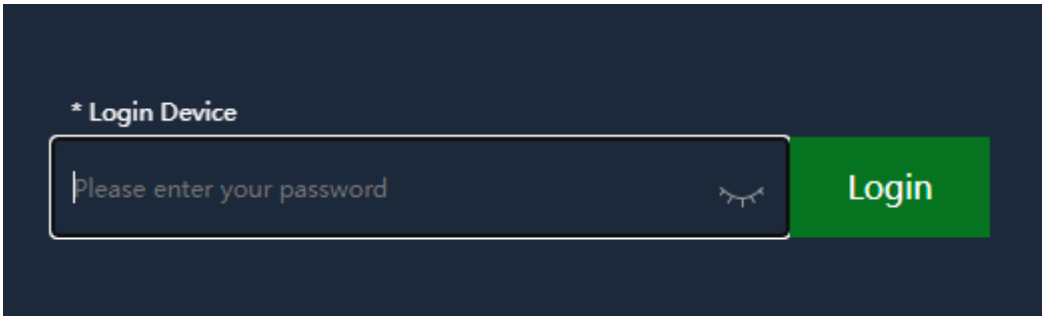


Figure 4-6 Login Window

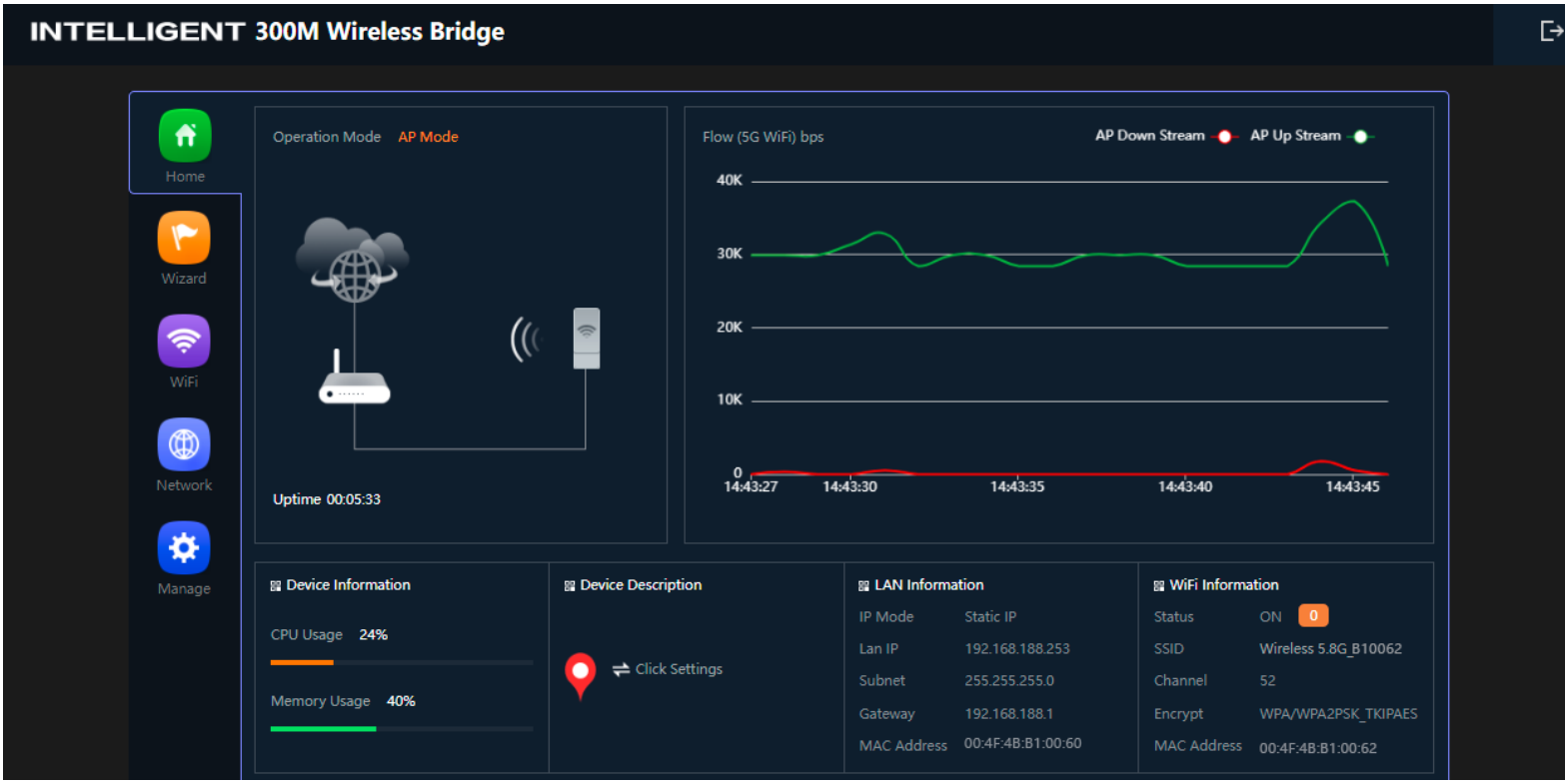
Default IP Address: **192.168.1.253**

Default ID/Password: **admin**

If the above screen does not pop up, it may mean that your web-browser has been set to a proxy. Go to Tools menu> Internet Options> Connections> LAN Settings on the screen that appears, uncheck **Using Proxy** and click **OK** to finish it.

Chapter 5. Configuring the CPE

This chapter delivers a detailed presentation of CPE's functionalities and features 3 main items below, allowing you to manage the CPE with ease. The screen shots use the AirMax5X II as an example.



The page includes the following fields:

Object	Description
Operation Mode	It shows the current mode status.
Device Information	It shows the CPU/memory usage.
Device Description	You can enter the device description.
Flow (2.4G/5G Wi-Fi) bps	It shows the Upstream/Downstream graph.
LAN Information	It shows the device IP mode, LAN IP, subnet, gateway and MAC address.
Wi-Fi Information	It shows the Wi-Fi status, SSID, channel, Encryption, MAC address and client list.
Version	It shows the firmware version (Double-click to show more detailed info.).

5.1 Wizard

The Wizard guides you to configuring the AirMax5X II in a different mode, including AP ,Repeater mode.

Figure 5-2 Operation Mode

The default operation mode is AP mode.

Change the PtP switch to optional AP/repeater mode.

5.2 AP Mode

Click "**Wizard**" → "**AP Mode**" and the following page will be displayed. This section allows you to configure the AP mode.

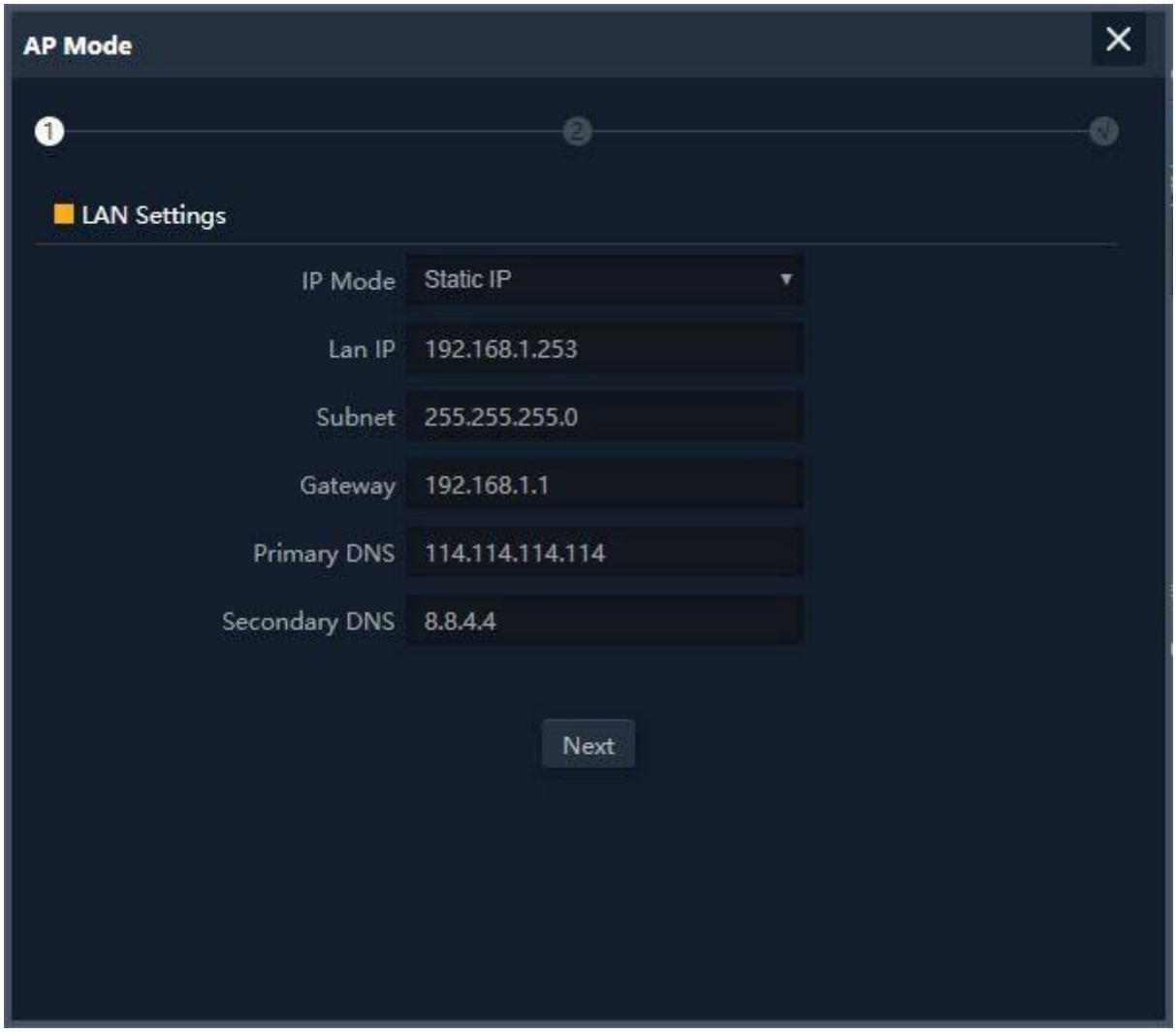


Figure 5-2 AP Mode

The page includes the following fields:

Object	Description
IP Mode	Select "**Static IP**" or "**DHCP Client**" for setting up device IP
LAN IP	Enter the AP static IP address
Subnet	Enter the network mask
Gateway	Enter the default gateway IP address
Primary DNS	Enter the primary DNS IP address, or not insert ip address
Secondary DNS	Enter the secondary DNS IP address, or not insert the ip address

Figure 5-21 AP Mode – Set up Wi-Fi The page includes the following fields:

Object	Description
Wi-Fi Status	Select **ON (Green)** or **OFF (Gray)** to enable or disable wireless LAN
SSID	It is the wireless network name. The default SSID is "**AirLive_2.4G**" or "**AirLive_5G**"
Hide your SSID ?	Select **ON** (**Green**) or **OFF** (**Gray**) to hide wireless LAN or not
Bandwidth	Select the operating channel width, "**20MHz**" or "**40MHz**" or **80MHz**"
Channel	Select the operating channel you would like to use. The channel range will be changed by selecting a different domain.
Encryption	Select the wireless encryption. The default is "**None**"
Timing	Set time to restart

5.3 Repeater Mode

Click “**Wizard**” → “**Repeater Mode**” and the following page will be displayed. This section allows you to configure the Repeater mode.

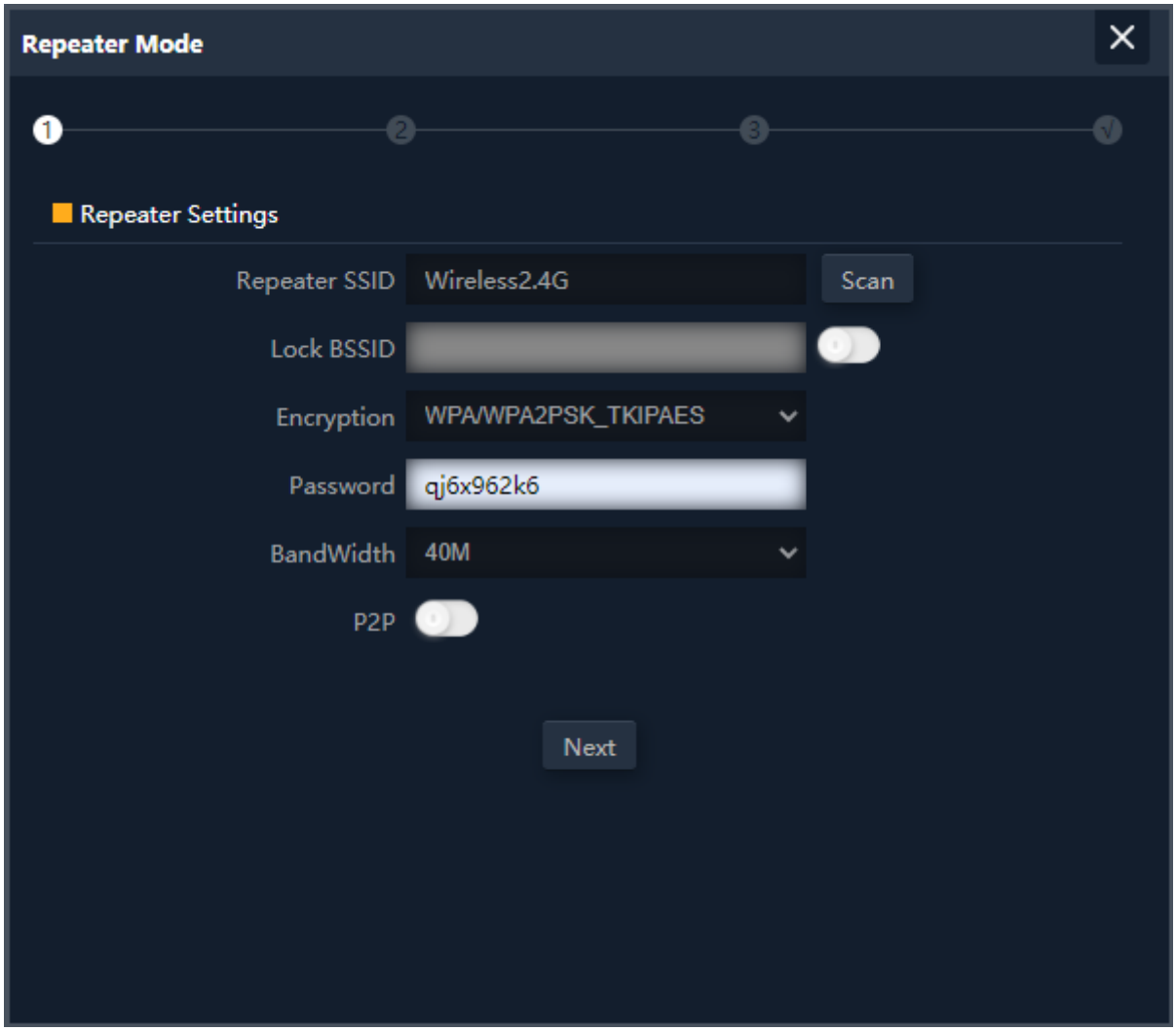


Figure 5-3 Repeater Mode The page includes the following fields:

Object	Description
Repeater SSID	Enter the root AP’s SSID or press “**Scan**” to select
Lock BSSID	Check to lock the root AP’ MAC address
Encryption	Select the wireless encryption of root AP. The default is “**WPA/WPA2PSK_TKIPAES**”
Password	Enter the password of root AP
Bandwidth	Select the operating channel width, “**20MHz**” or “**40MHz**” or “**80MHz**”
P2P	Enable switch for Point to Point function

Press the "**Scan"** button to find the root AP that you need to repeat and press **Choice** to select the AP.

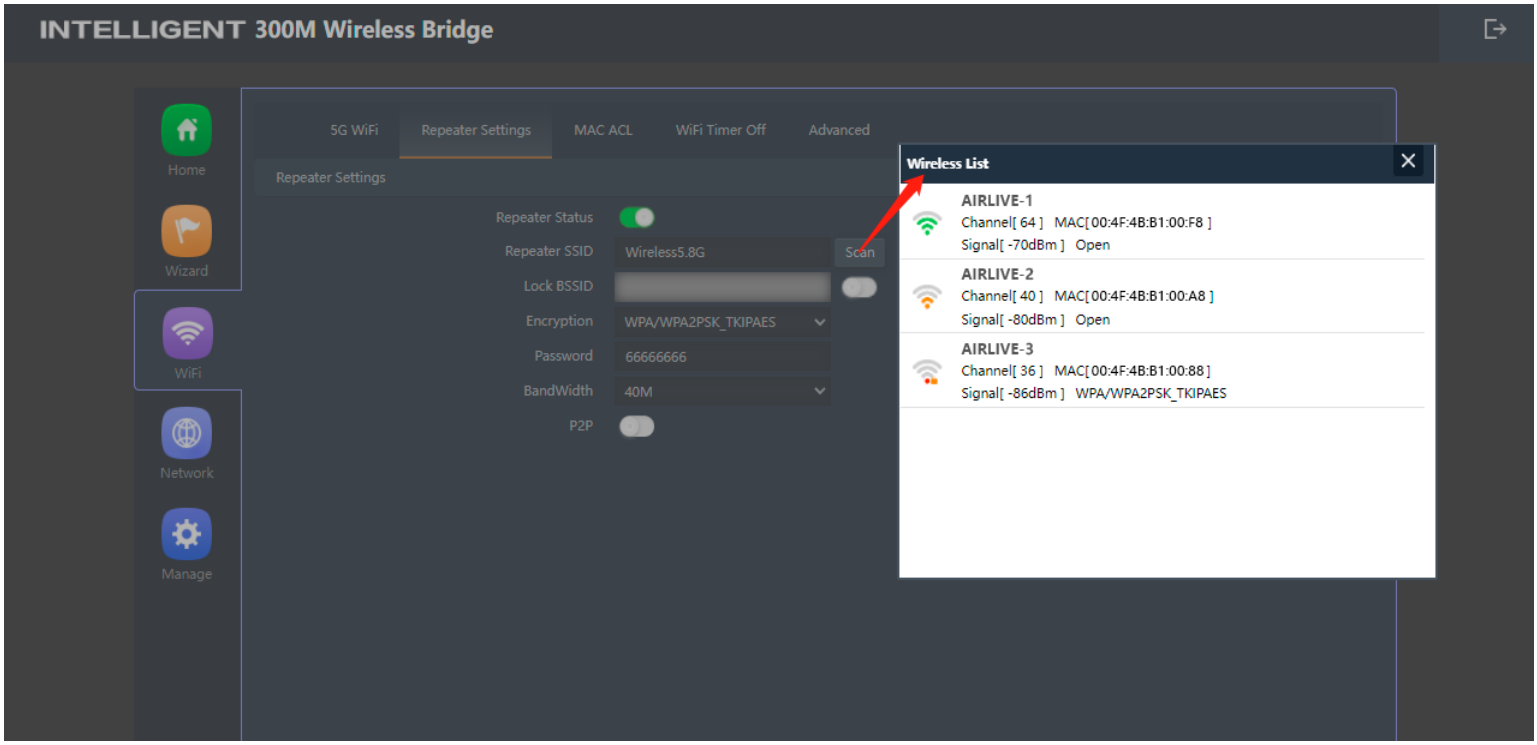


Figure 5-32 Repeater Mode -- Scan AP

Set up the repeater wireless network

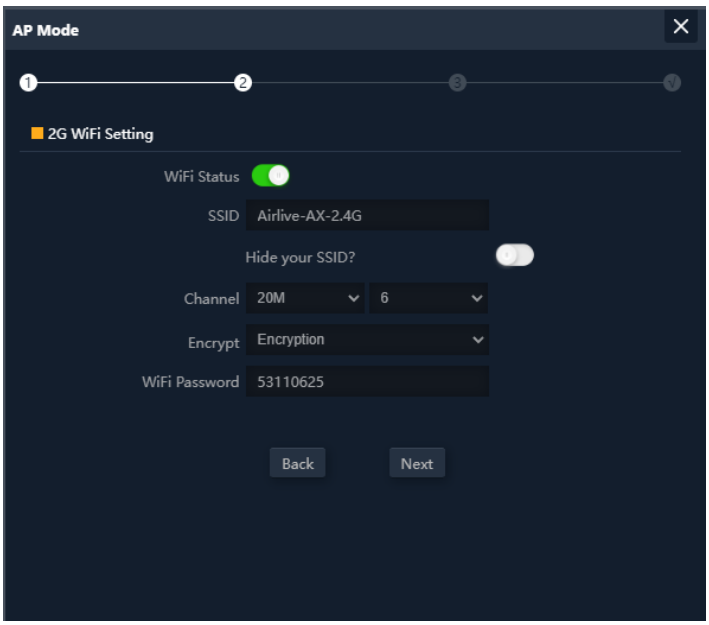


Figure 5-20 Repeater Mode – Setting up Wi-Fi The page includes the following fields:

Object	Description
Wi-Fi Status	Select **ON (Green)** or **OFF (Gray)** to enable or disable wireless LAN
SSID	It is the wireless network name. The default SSID is "**AirLive_2.4G**" or "**AirLive_5G**"
Hide your SSID ?	Select **ON** (**Green**) or **OFF** (**Gray**) to hide wireless LAN or not
Encryption	Select the wireless encryption. The default is "**None**"
Timing	Set time to restart

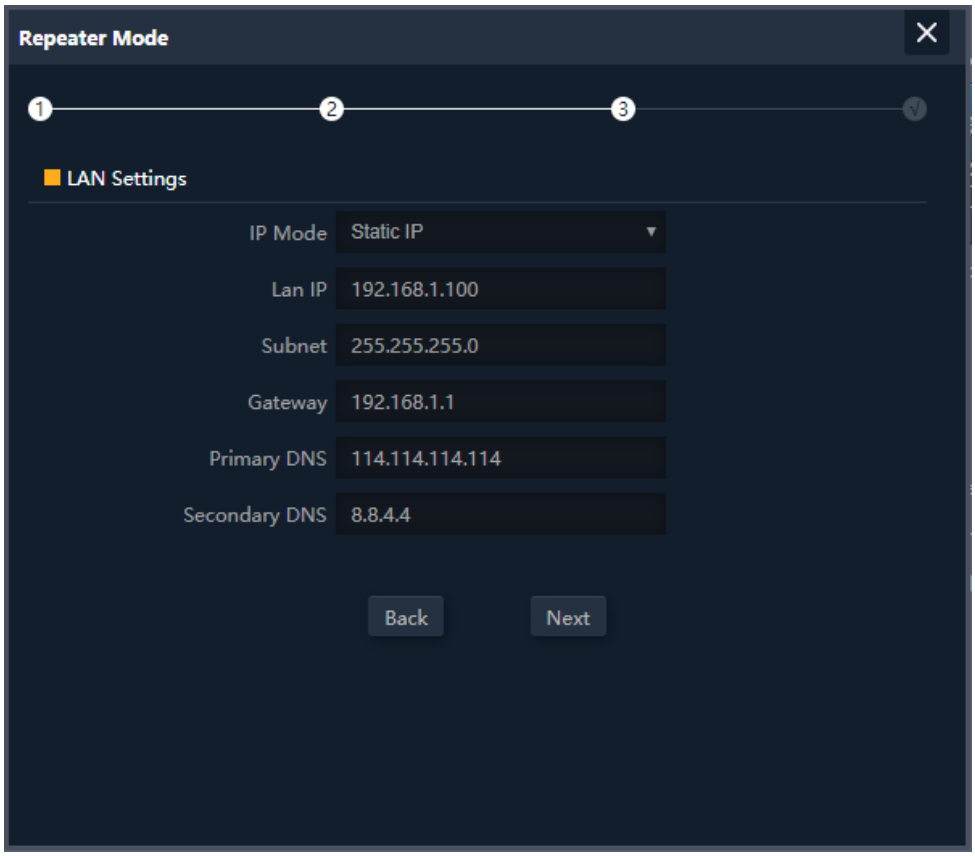


Figure 5-33 Repeater Mode – Setting up Wi-Fi

The page includes the following fields:

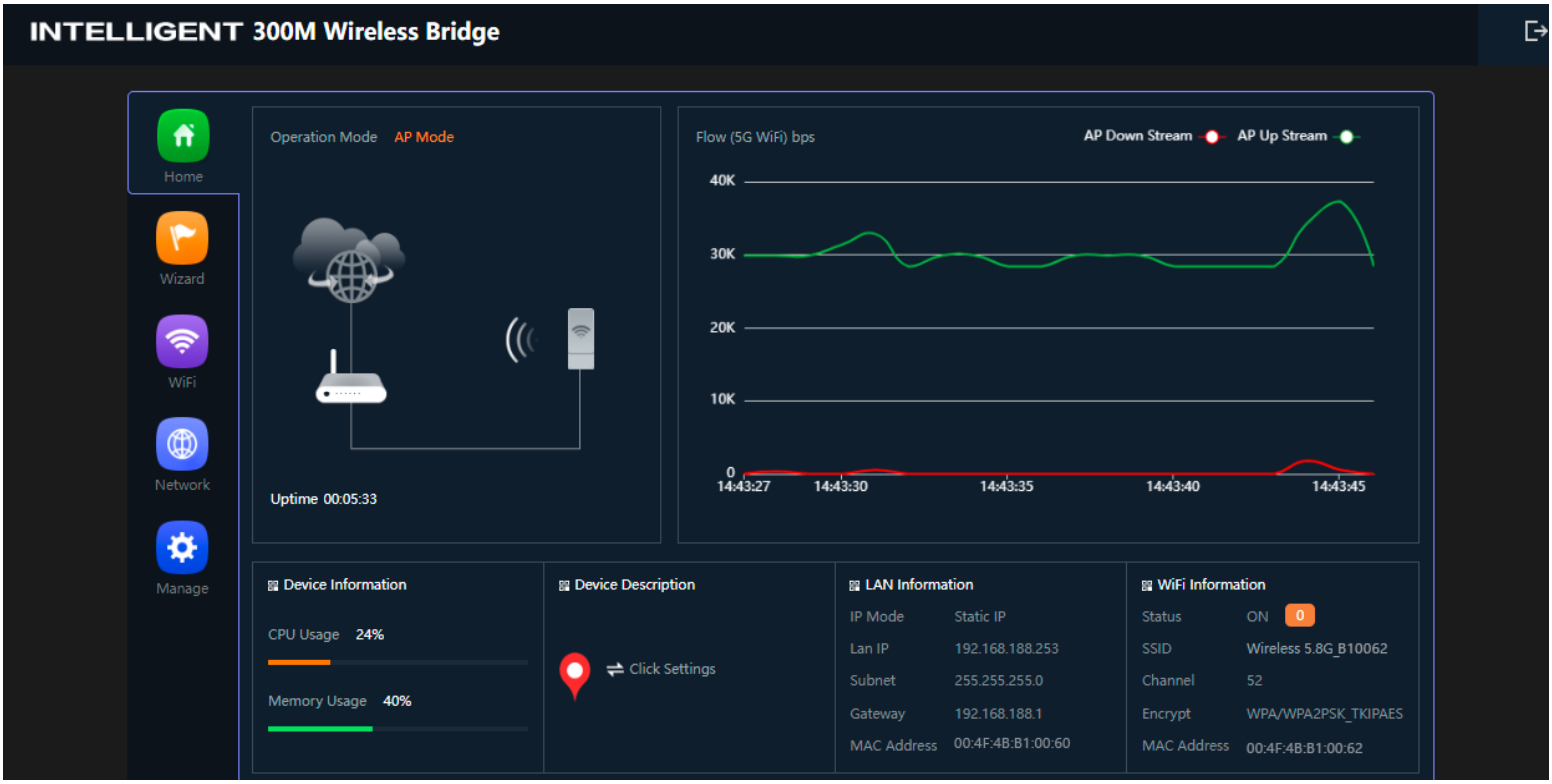
Object	Description
IP Mode	Select "**Static IP**" or "**DHCP Client**" for setting up device IP
LAN IP	Enter the AP static IP address
Subnet	Enter the network mask
Gateway	Enter the default gateway IP address
Primary DNS	Enter the primary DNS IP address, or not
Secondary DNS	Enter the secondary DNS IP address, or not

Enter the LAN IP address.

5.4 Wi-Fi

2.4G/5G Wi-Fi

5.4.1 Basic



Object	Description
Wi-Fi Status	Select **ON (Green)** or **OFF (Gray)** to enable or disable wireless LAN
SSID	It is the wireless network name. The default SSID is "**AirLive_2.4G**" or "**AirLive_5G**"
Hide your SSID ?	Select **ON** (**Green**) or **OFF** (**Gray**) to hide wireless LAN or not
Channel	It shows the channel of the CPE. Default 2.4G channel is 6, and 5GHz is channel 36.
Encryption	Select the wireless encryption. The default is "**None**"
WMM	Enable/Disable WMM (Wi-Fi Multimedia) function
Wi-Fi Analyzer	Press this button to analyze local area wireless signal

5.4.2 VAP

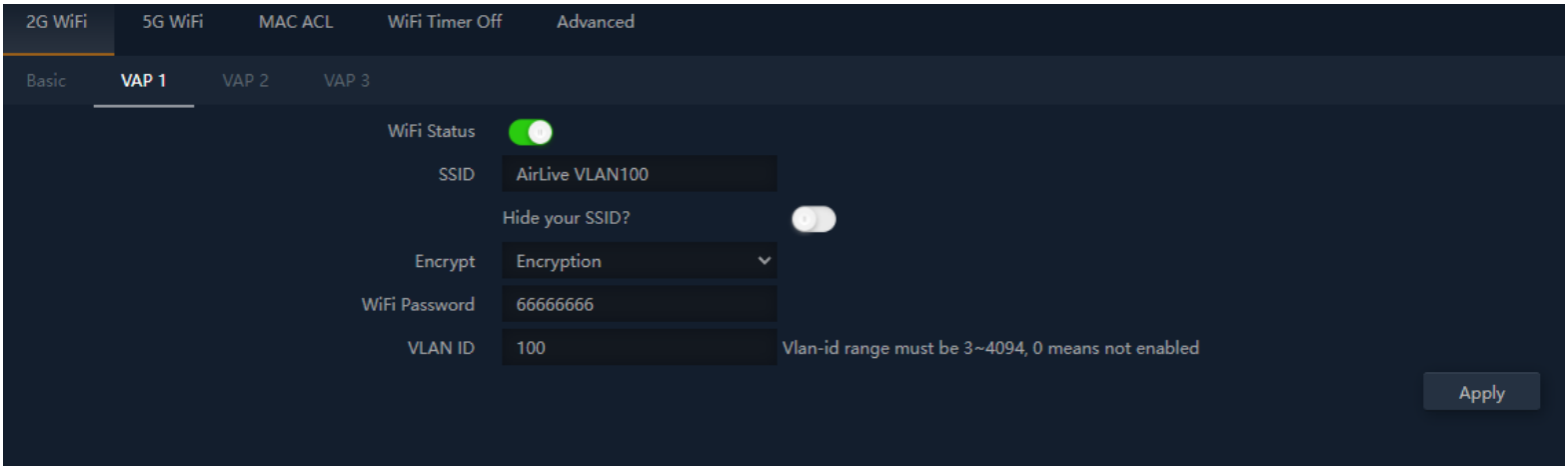


Figure 5-23 VAP

Select VAP1~VAP3 to enable virtual AP

The page includes the following fields:

Object	Description
Wi-Fi Status	Select **ON (Green)** or **OFF (Gray)** to enable or disable virtual wireless LAN
SSID	It is the wireless network name. The default SSID is "**AirLive_2.4G_1**" to **AirLive_2.4G_3**" or "**AirLive_5G_1**" to **AirLive_5G_3**"
Hide your SSID ?	Select **ON** (**Green**) or **OFF** (**Gray**) to hide wireless LAN or not
Channel	It shows the channel of the CPE. Default 2.4GHz is channel 6, and 5GHz is channel 36.
Encryption	Select the wireless encryption. The default is "**None**"
WMM	Enable/Disable WMM (Wi-Fi Multimedia) function

MAC ACL

5.4.3 MAC ACL=MAC Access Control List

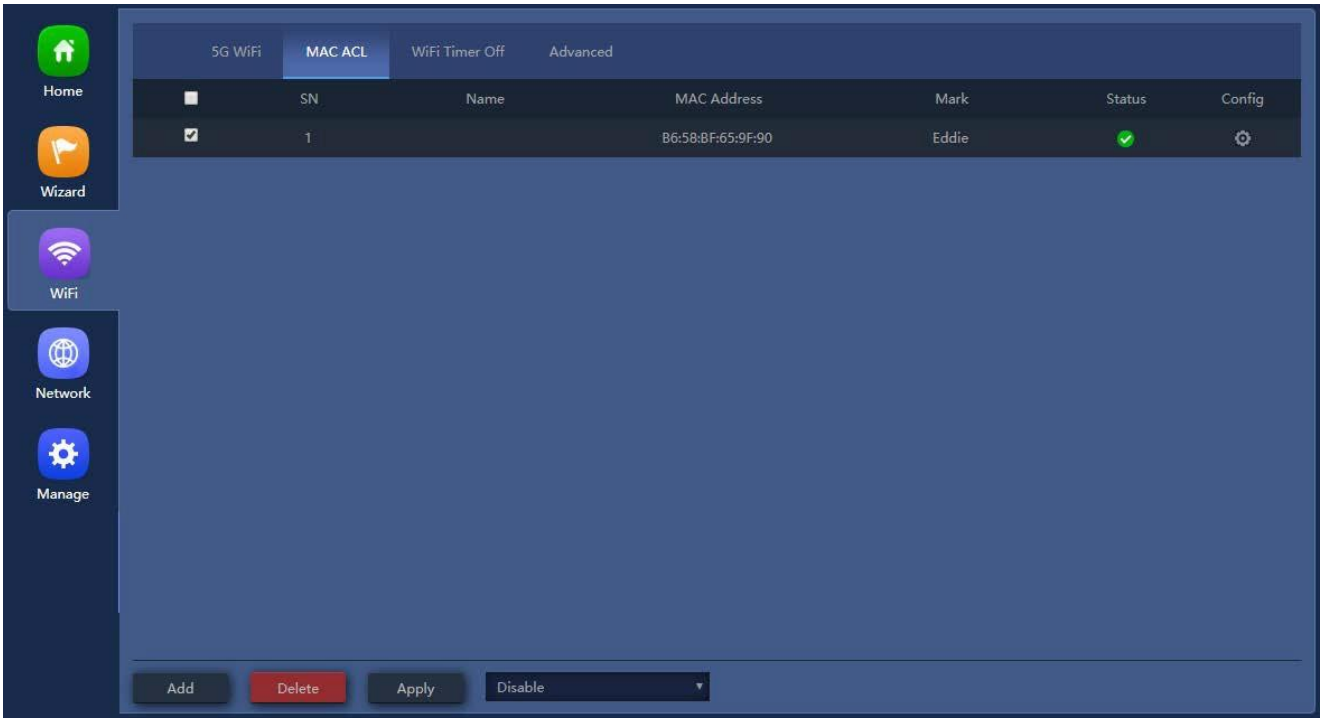


Figure 5-104 MAC ACL

The page includes the following fields:

Object	Description
Add	Press the "**Add**" button to add end-device that is scanned from wireless network and mark them
Delete	Press the "**Delete**" button to delete device from list
Apply	Press the "**Apply**" button to enable/disable the rule
ACL Status	Select the rule of ACL, default is **Disable**. Whitelist: **Allows the devices to pass in the rule** Blacklist: **Prohibited rules within the device through**

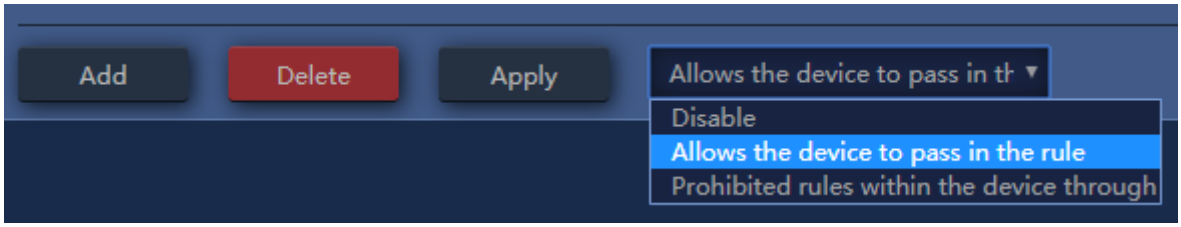


Figure 5-25 ACL status

Wi-Fi Timer Off

5.4.4 Wi-Fi Timer Off

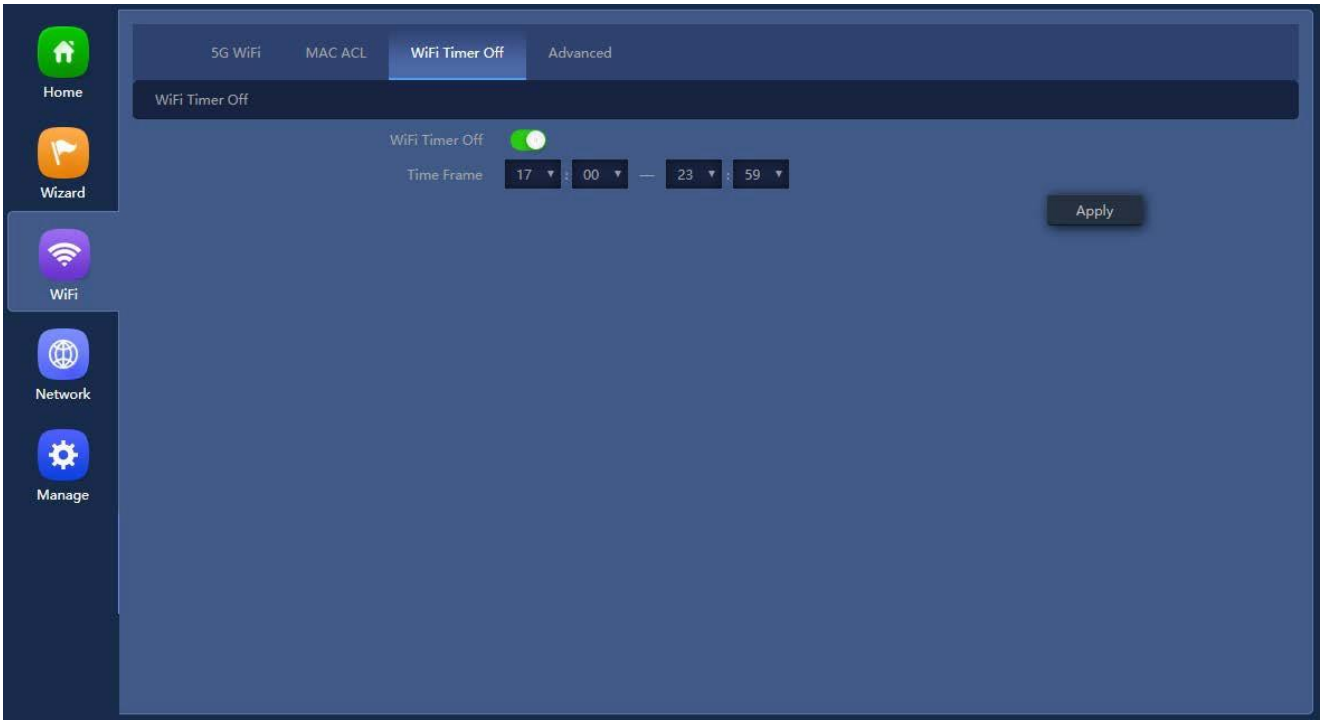


Figure 5-26 Wi-Fi Timer Off

The page includes the following fields:

Object	Description
Wi-Fi Timer Off	Select ON (**Green**) or OFF (**Gray**) to enable or disable timer
Time Frame	Choose the time frame of Wi-Fi

Advanced

5.4.5 Advanced

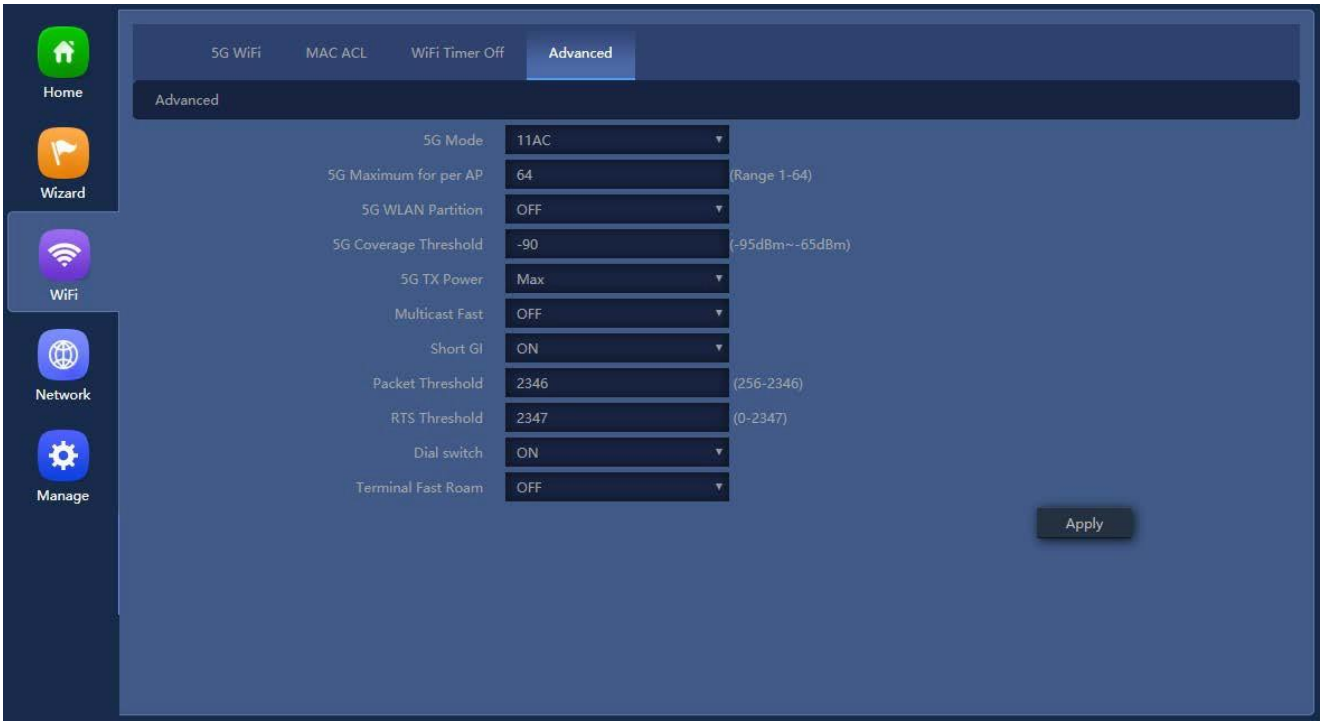


Figure 5-27 Advanced The page includes the following fields:

Object	Description
2.4G/5G Mode	Select **802.11A** or **802.11AN** or **802.11AC** in CPE
Maximum 2.4G/5G per AP	The maximum users are **64** per radio
2.4G/5G WLAN Partition	Enable it to isolate each connected wireless client so that they cannot access mutually.
2.4G/5G Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -90dBm
2.4G/5G TX Power	The range of transmit power is **Max (100%)**, **Efficient (75%)**, **Enhanced (50%), Standard (25%)** or **Min (12.5%)**. In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power
Multicast Fast	A part of the 802.11n standard that allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source, destination end points, and traffic class (QoS) into one large frame with a common MAC header
Short GI	Guard intervals are used to ensure that distinct transmissions do not interfere with one another.
Packet Threshold	When the length of a d ata packet exceeds this value, the router will

	send an RTS frame to the destination wireless node, and the latter will reply with a CTS frame, and thus they are ready to communicate. The default value is **2346**
RTS Threshold	Enable or Disable RTS/CTS protocol. It can be used in the following scenarios and used by Stations or Wireless AP. 1)When medium is too noisy or lots of interferences are present. If the AP/Station cannot get a chance to send a packet, the RTS/CTS mechanism can be initiated to get the packet sent. 2)In mixed mode, the hidden node problem can be avoided. The default value is **2347**
Dial Switch	Enable or Disable physical PtP switch
Terminal Fast Roam	Enable or Disable 802.11k, 802.11v and 802.11r

5.5 Network

5.5.1 LAN Settings

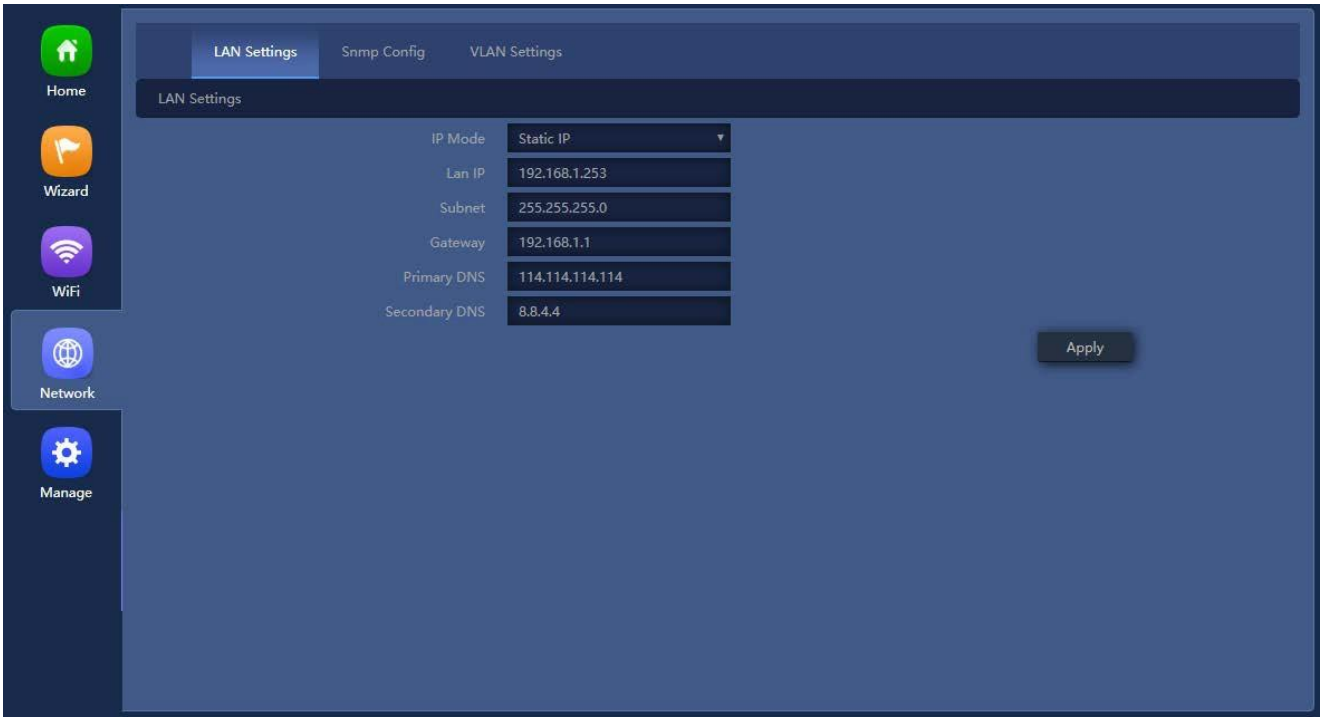


Figure 5-28 LAN Settings The page includes the following fields:

Object	Description
IP Mode	Select "**Static IP**" or "**DHCP Client**" for setting up device IP
LAN IP	Enter the AP static IP address
Subnet	Enter the network mask
Gateway	Enter the default gateway IP address
Primary DNS	Enter the primary DNS IP address, or not
Secondary DNS	Enter the secondary DNS IP address, or not

5.5.2 SNMP Config

Figure 5-29 SNMP Config

The page includes the following fields:

Object	Description
Read Community	Enter the read community, default is **public**
Write Community	Enter the write community, default is **private**
Trap Destination Address	Enter the SNMP trap IP address, default is **192.168.1.100**

5.5.3 VLAN Settings

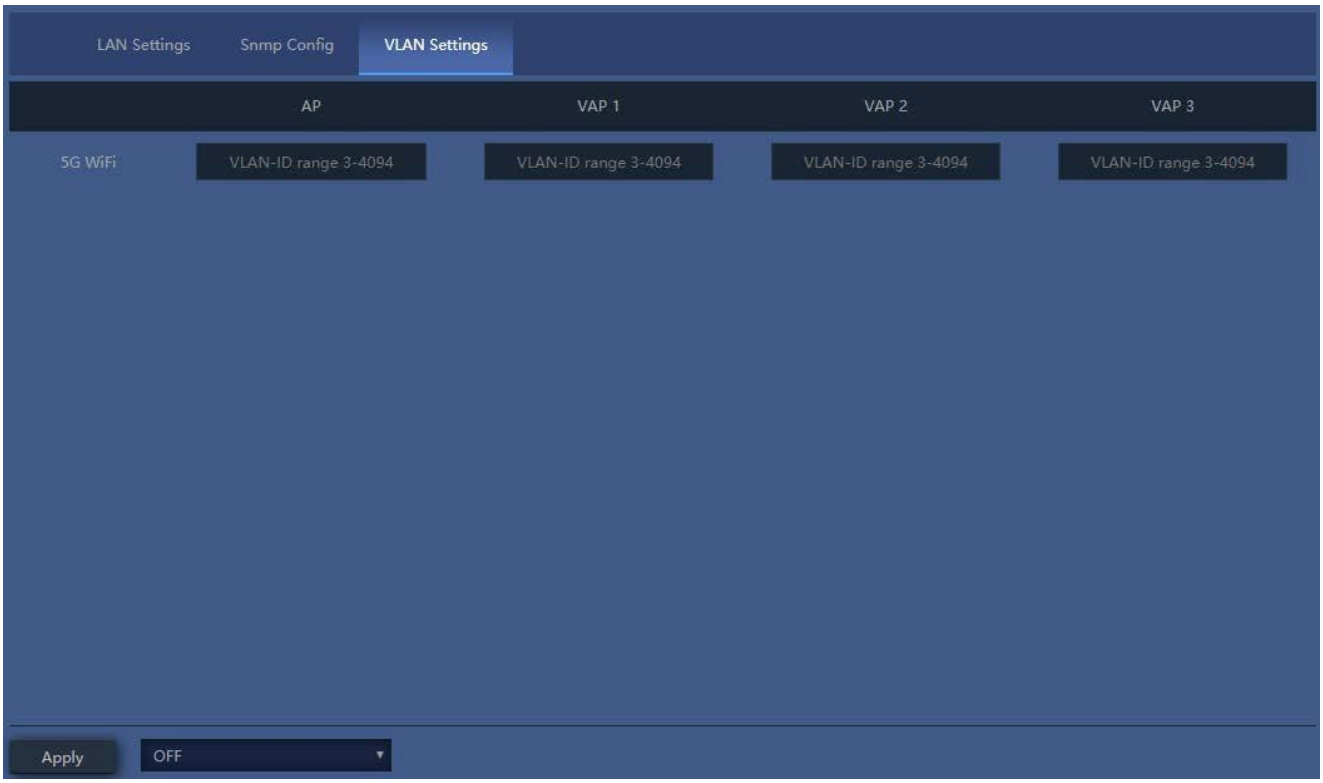


Figure 5-11 VLAN Settings

The page includes the following fields:

Object	Description
AP	Select AP or VAP included in the VLAN
VLAN ID	Enter the VLAN ID from 3 to 4094

5.5.4 WAN Settings

Static IP

If your ISP offers you static IP Internet connection type, select "**Static IP**" and then enter IP address, subnet mask, default gateway and primary DNS information provided by your ISP in the corresponding fields.

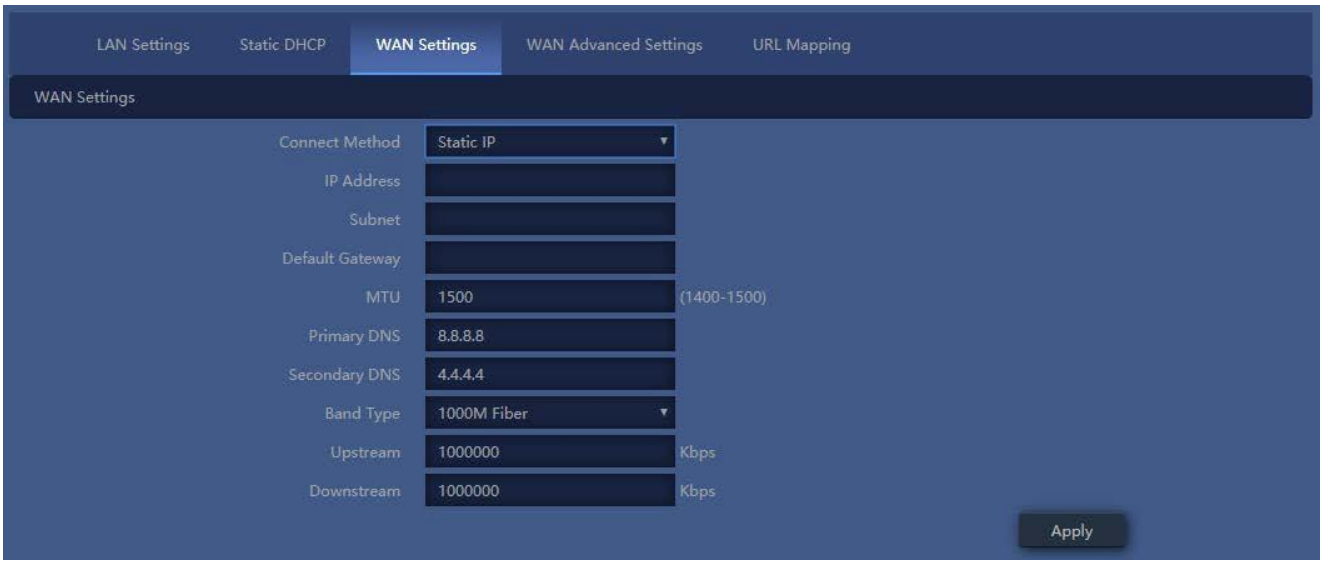


Figure 5-31 Static IP

The page includes the following fields:

Object	Description
IP Address	Enter the WAN IP address provided by your ISP. Enquire your ISP if you are not clear
Subnet	Enter WAN Subnet Mask provided by your ISP
Default Gateway	Enter the WAN Gateway address provided by your ISP
MTU	Maximum Transmission Unit. Default is 1500
Primary DNS	Enter the necessary DNS address provided by your ISP
Secondary DNS	Enter the secondary DNS address provided by your ISP
Upstream	Enter limited upstream throughput, default is **1000000** Kbps
Downstream	Enter limited downstream throughput, default is **1000000** Kbps

PPPoE (ADSL)

Select **PPPOE** if your ISP is using a PPPoE connection and provide you with PPPoE user name and password info.

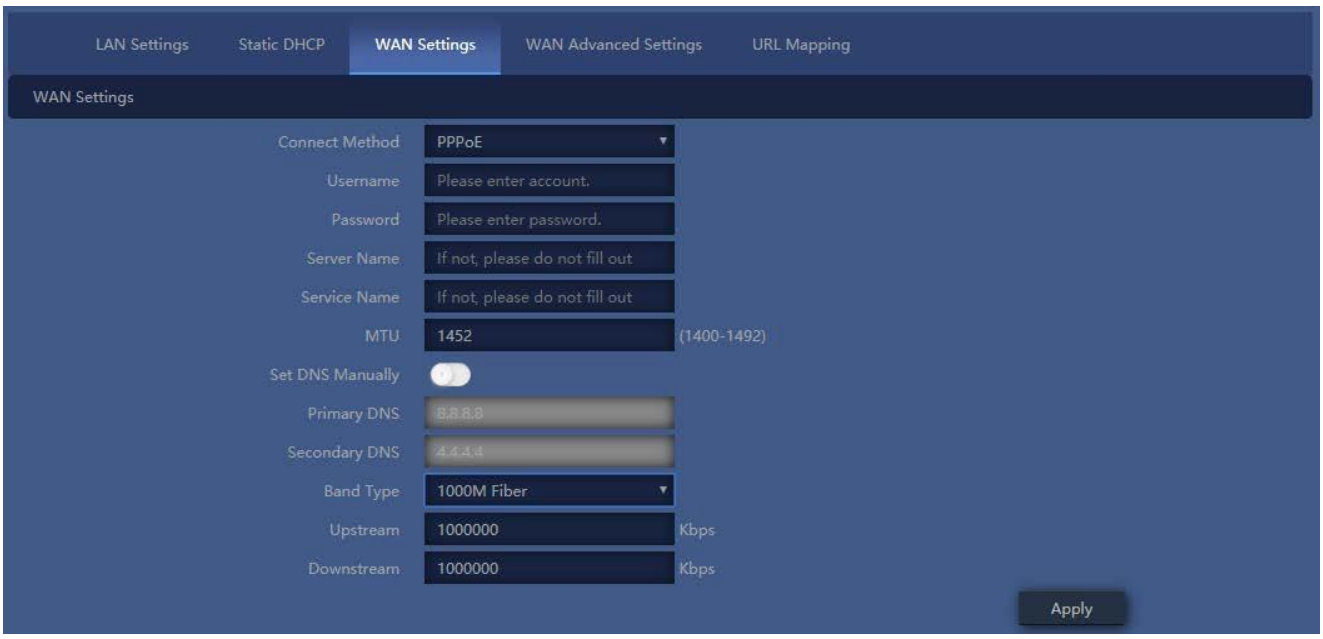


Figure 5-32 PPPoE (ADSL) The page includes the following fields:

Object	Description
Username	Enter the PPPoE User Name provided by your ISP
Password	Enter the PPPoE password provided by your ISP
Set DNS Manually	Enable/Disable DNS Manually
Primary DNS	Enter the necessary DNS address provided by your ISP
Secondary DNS	Enter the secondary DNS address provided by your ISP
MTU	Maximum Transmission Unit. Default is 1452
Band Type	Select the band type provided by your ISP
Upstream	Enter limited upstream throughput, default is **1000000** Kbps
Downstream	Enter limited downstream throughput, default is **1000000** Kbps

DHCP

Choose "**DHCP**" and the router will automatically obtain IP addresses, subnet masks and gateway addresses from your ISP.

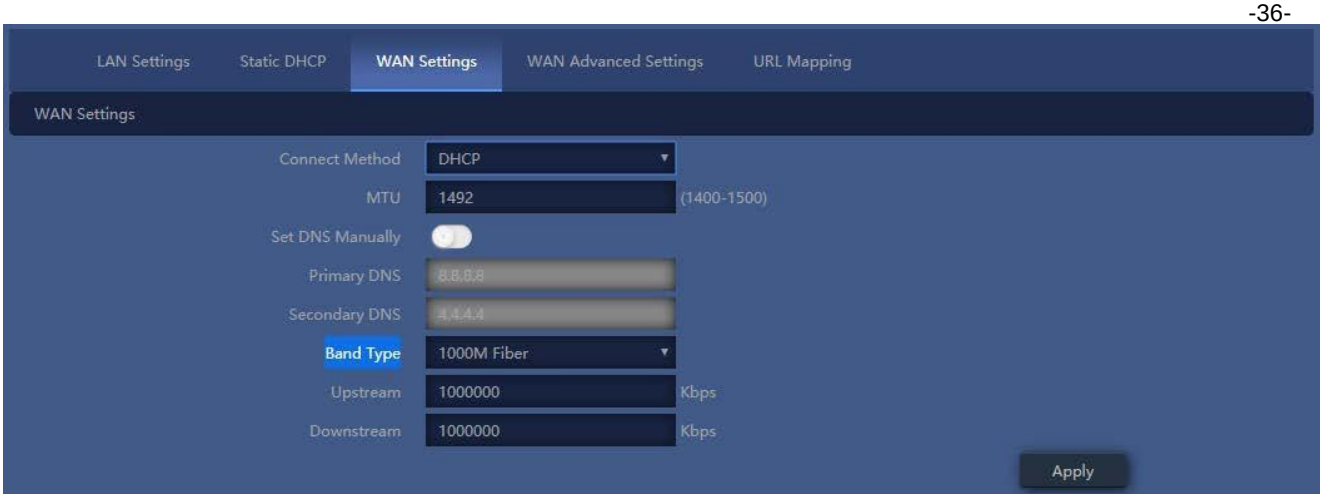


Figure 5-12 DHCP

The page includes the following fields:

Object	Description
MTU	Maximum Transmission Unit. Default is 1452
Set DNS Manually	Enable/Disable DNS Manually
Primary DNS	Enter the necessary DNS address provided by your ISP
Secondary DNS	Enter the secondary DNS address provided by your ISP
Band Type	Select the band type provided by your ISP
Upstream	Enter limited upstream throughput, default is **1000000** Kbps
Downstream	Enter limited downstream throughput, default is **1000000** Kbps

5.5.5 WAN advanced settings

Figure 5-13 WAN advanced settings

The page includes the following fields:

Object	Description
Enable web server access on WAN port	Enable to access from WAN, default port is 8080
MAC clone	Enable and scan to clone the MAC address
Enable Ping Access on WAN	Enable or Disable this function
Enable IPsec passthrough on VPN connection	Enable or disable IPSec to pass through IPSec communication data.
Enable PPTP passthrough on VPN connection	Enable or disable PPTP to pass through PPTP communication data.
Enable L2TP passthrough on VPN connection	Enable or disable L2TP to pass through L2TP communication data.
Line Detection	Enable to ping Host 1 and Host 2 IP. If ping fails, the WAN will be disconnected.

5.6 Security

5.6.1 URL Filtering

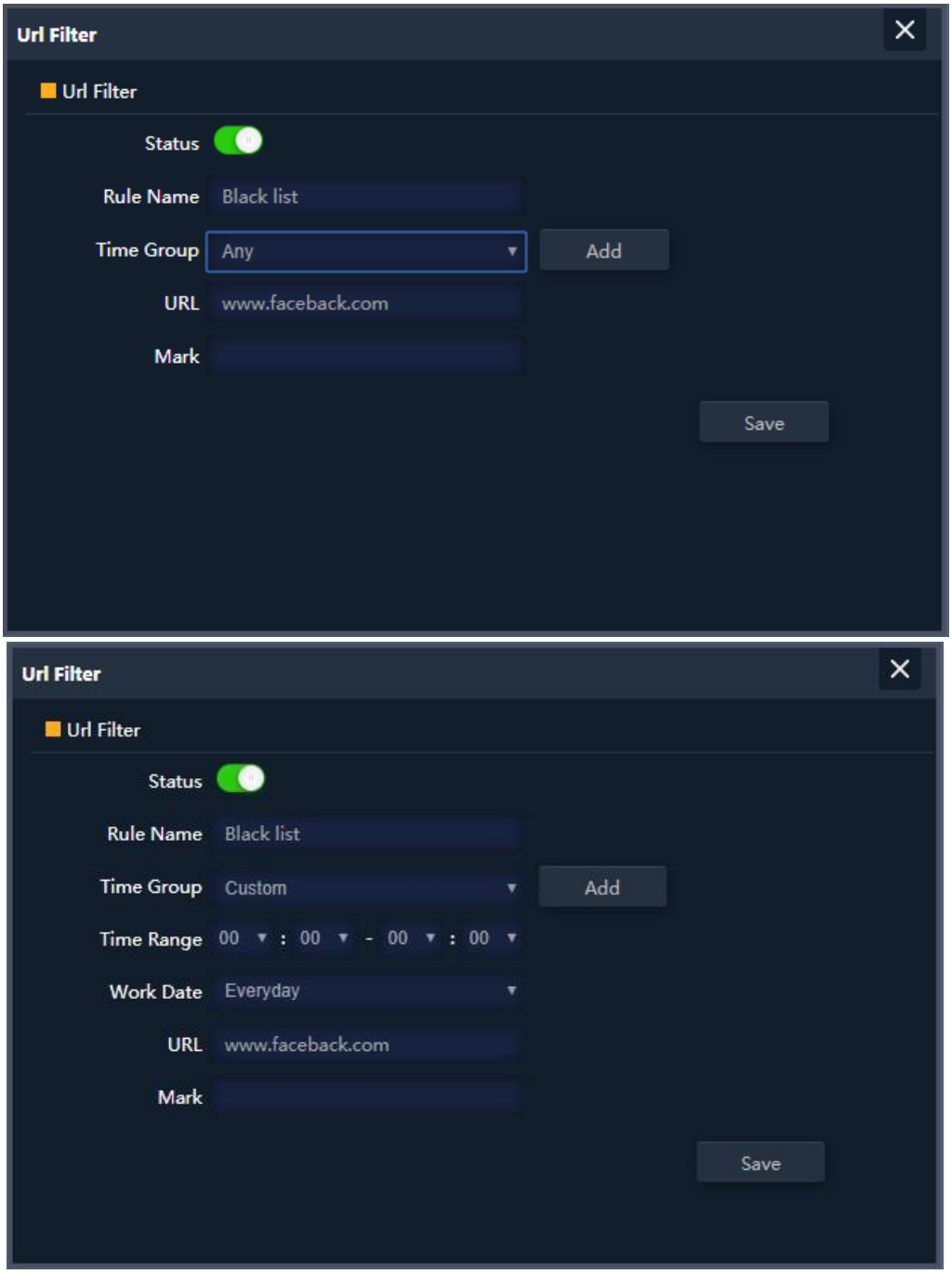


Figure 5-35 URL Filtering

The page includes the following fields:

Object	Description
Add	Press the "**Add**" button to add the rule
Delete	Press the "**Delete**" button to delete the rule

Apply	Press the "**Apply**" button to enable/disable the rule
Status	Select **ON (Green)** or **OFF (Gray)** to enable or disable
Rule Name	Enter the rule name, e.g. Black list
Time Group	Select **Any** or **Customer** to set up time range and work data.
URL	Enter the URL that you need to put in Blacklist
Mark	Enter the mark string, or not

Enable/disable URL filter function

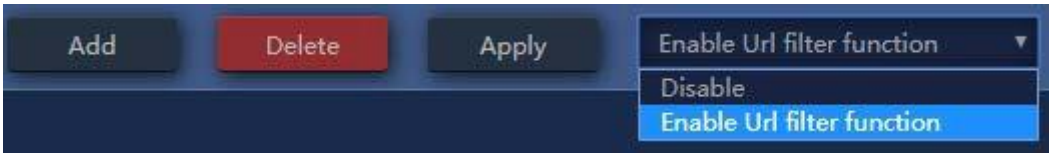


Figure 5-36 URL Filtering

5.6.2 IP/Port Filtering

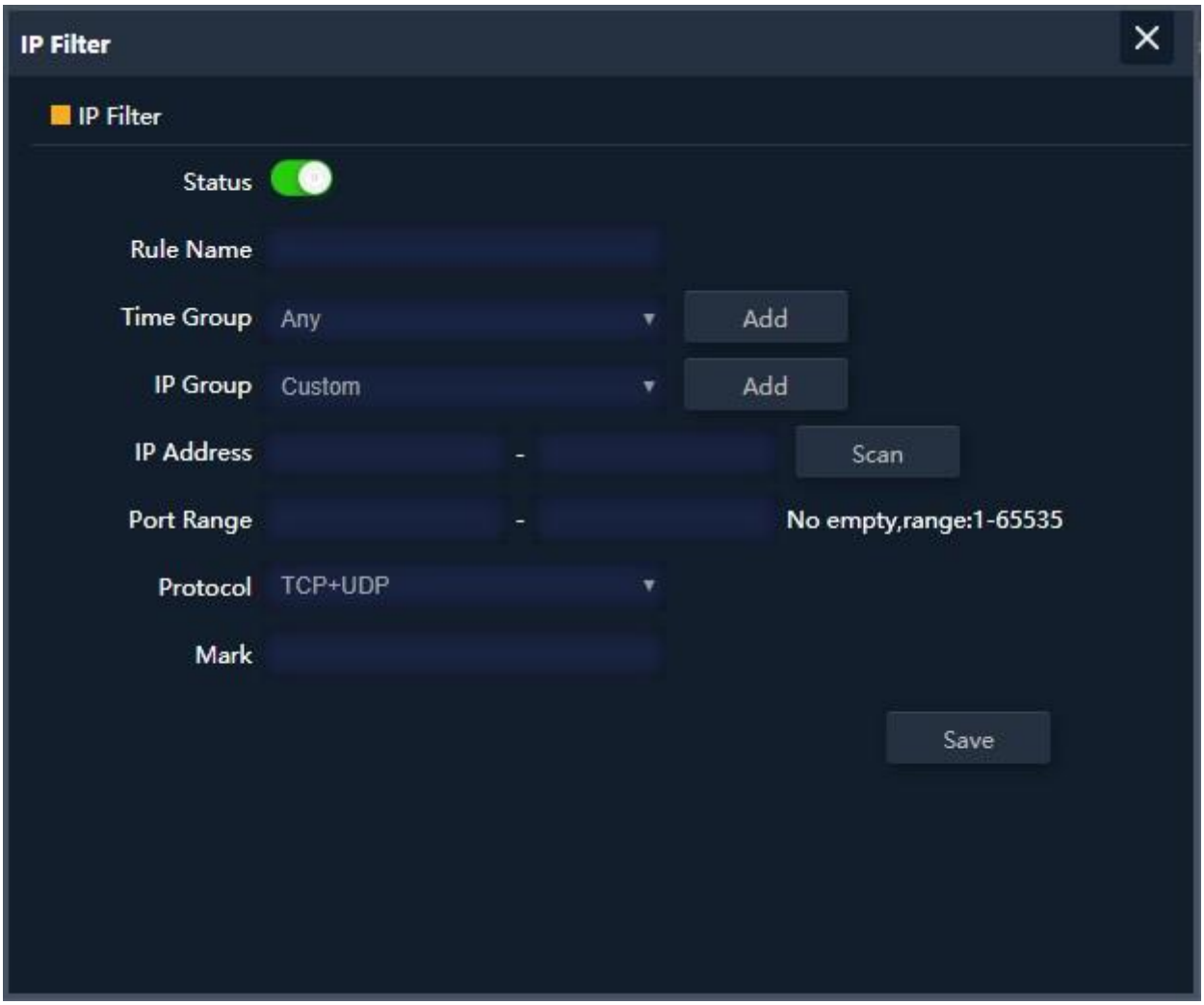


Figure 5-37 IP/Port Filtering

The page includes the following fields:

Object	Description
Add	Press the "**Add**" button to add the rule in the Black- or Whitelist
Delete	Press the "**Delete**" button to delete the rule
Apply	Press the "**Apply**" button to enable/disable the rule
Status	Select **ON (Green)** or **OFF (Gray)** to enable or disable
Rule Name	Enter the rule name, e.g. Black list
Time Group	Select **Any** or **Customer** to set up time range and work data.
IP Group	Select IP Group for adding IP by entering IP range or by scanning devices
IP Address	Enter the IP that you need to put in Black- or Whitelist
Port Range	Enter the web port to access
Protocol	Select **TCP**, **UDP** or **TCP+UDP**
Mark	Enter the mark string, or not
IP/Port Filtering Status	Select the rule of IP/Port Filtering, default is **Disable**. Whitelist: **Allow the devices to pass in the rule** Blacklist: **Prohibited rules within the device through**

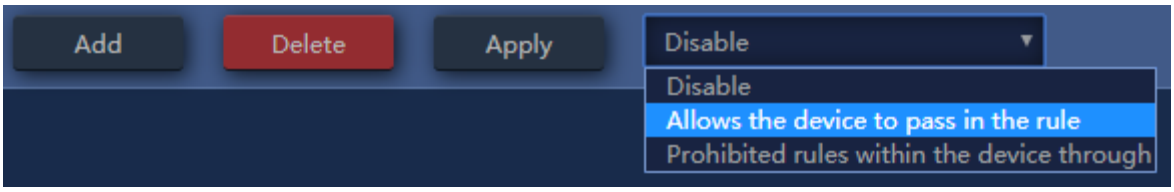


Figure 5-38 IP/Port Filtering

5.6.3 MAC Filtering

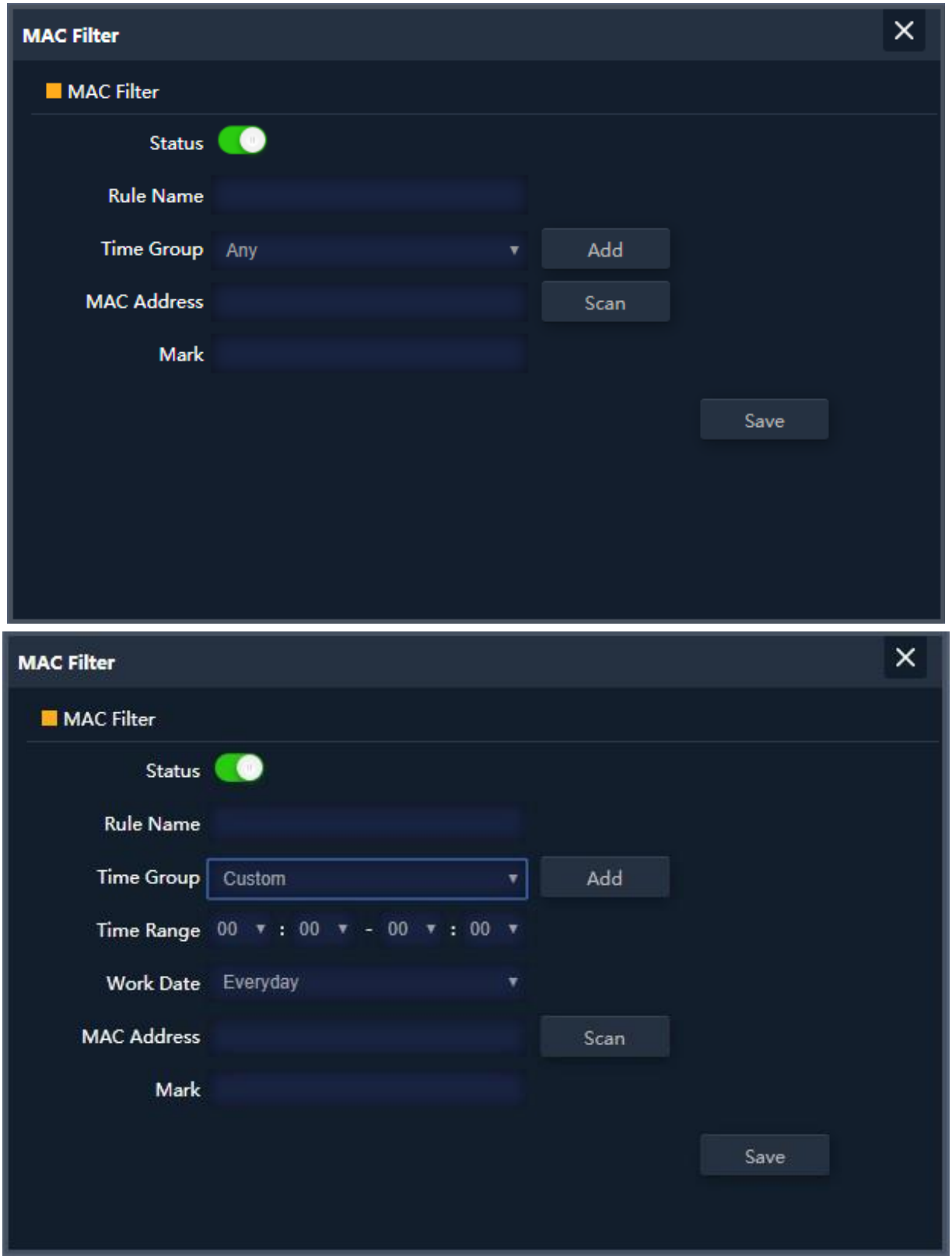


Figure 5-39 MAC Filtering

The page includes the following fields:

Object	Description
Add	Press the "**Add**" button to add the rule in the Black- or Whitelist
Delete	Press the "**Delete**" button to delete the rule
Apply	Press the "**Apply**" button to enable/disable the rule
Status	Select **ON (Green)** or **OFF (Gray)** to enable or disable
Rule Name	Enter the rule name, e.g. Black list
Time Group	Select **Any** or **Customer** to set up time range and work data.
MAC Address	Enter the MAC address that you need to put in Black- or Whitelist
Mark	Enter the mark string, or not
MAC Filtering Status	Select the rule of MAC Filtering, default is **Disable**. Whitelist: **Allow the devices to pass in the rule** Blacklist: **Prohibited rules within the device through**

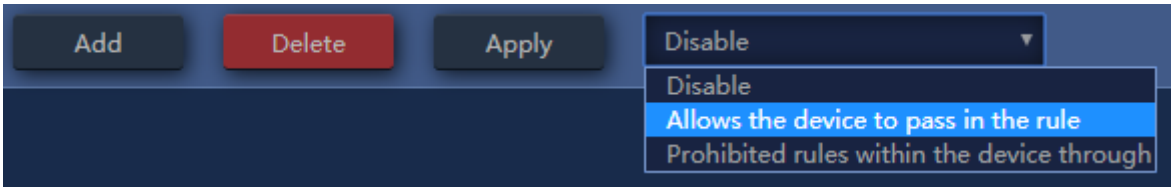


Figure 5-40 MAC Filtering

5.6.4 Security (Port Mapping/Port Forwarding)

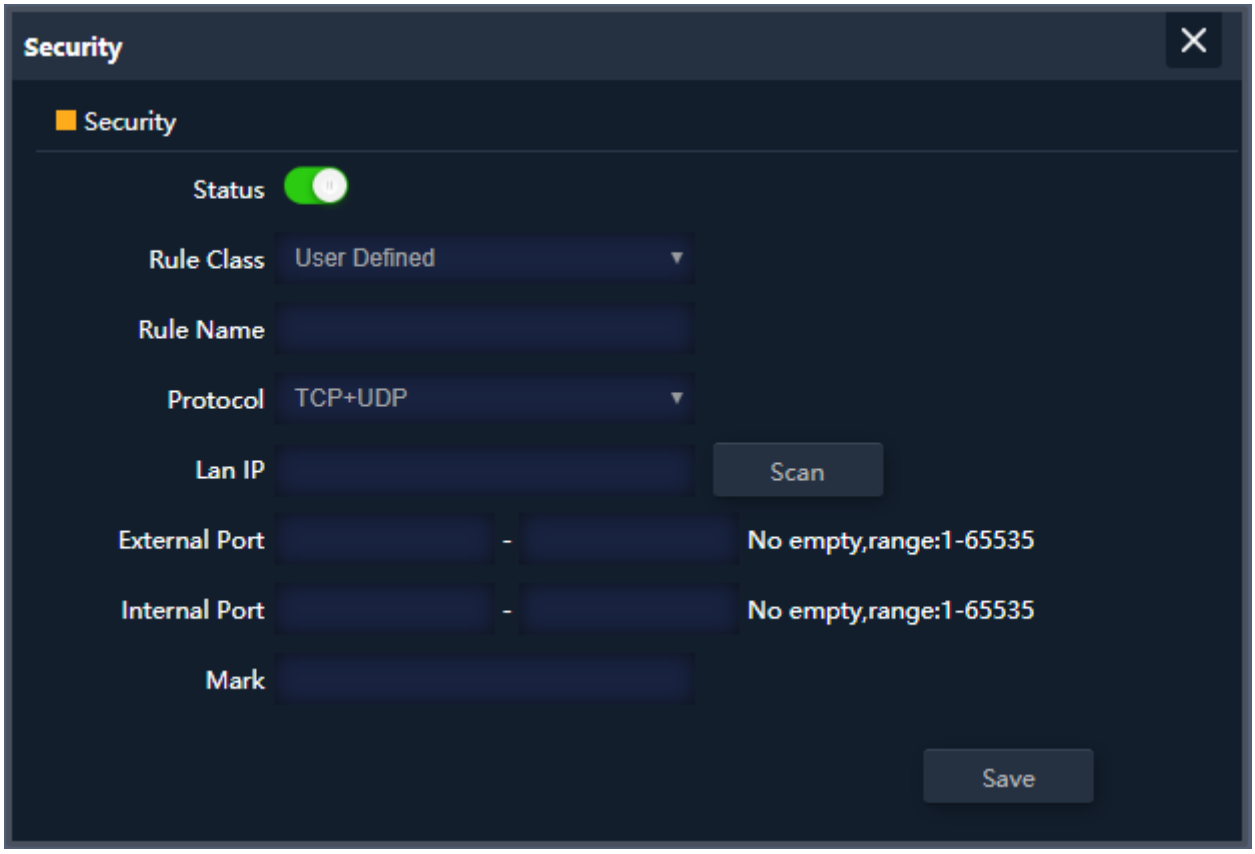


Figure 5-41 Port Mapping

The page includes the following fields:

Object	Description
Add	Press the "**Add**" button to add the rule in the black or white list
Delete	Press the "**Delete**" button to delete the rule
Apply	Press the "**Apply**" button to enable/disable the rule
Status	Select **ON (Green)** or **OFF (Gray)** to enable or disable
Rule Name	Enter the rule name, e.g. Black list
Protocol	Select **TCP**, **UDP** or **TCP+UDP**
LAN IP	Enter the IP address that you need for port forwarding
External Port	Enter the external port range
Internal Port	Enter the internal port range
Mark	Enter the mark string, or not

Enable/disable Port Mapping function

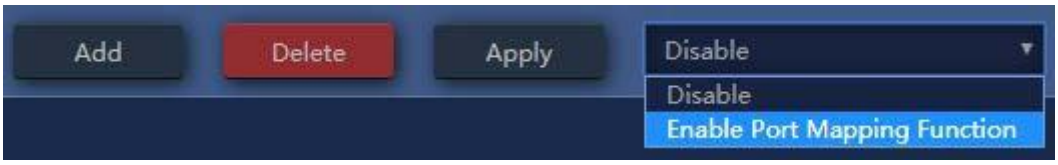


Figure 5-42 Port Mapping

5.6.5 DMZ

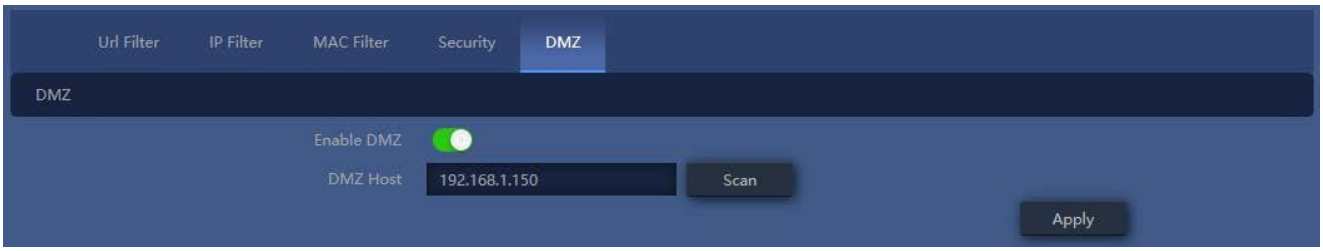


Figure 5-43 DMZ

The page includes the following fields:

Object	Description
Enable DMZ	Select **Enable DMZ Host** or **Disable**
DMZ Host IP	Enter the DMZ LAN IP

5.7 Manage

5.7.1 Configure

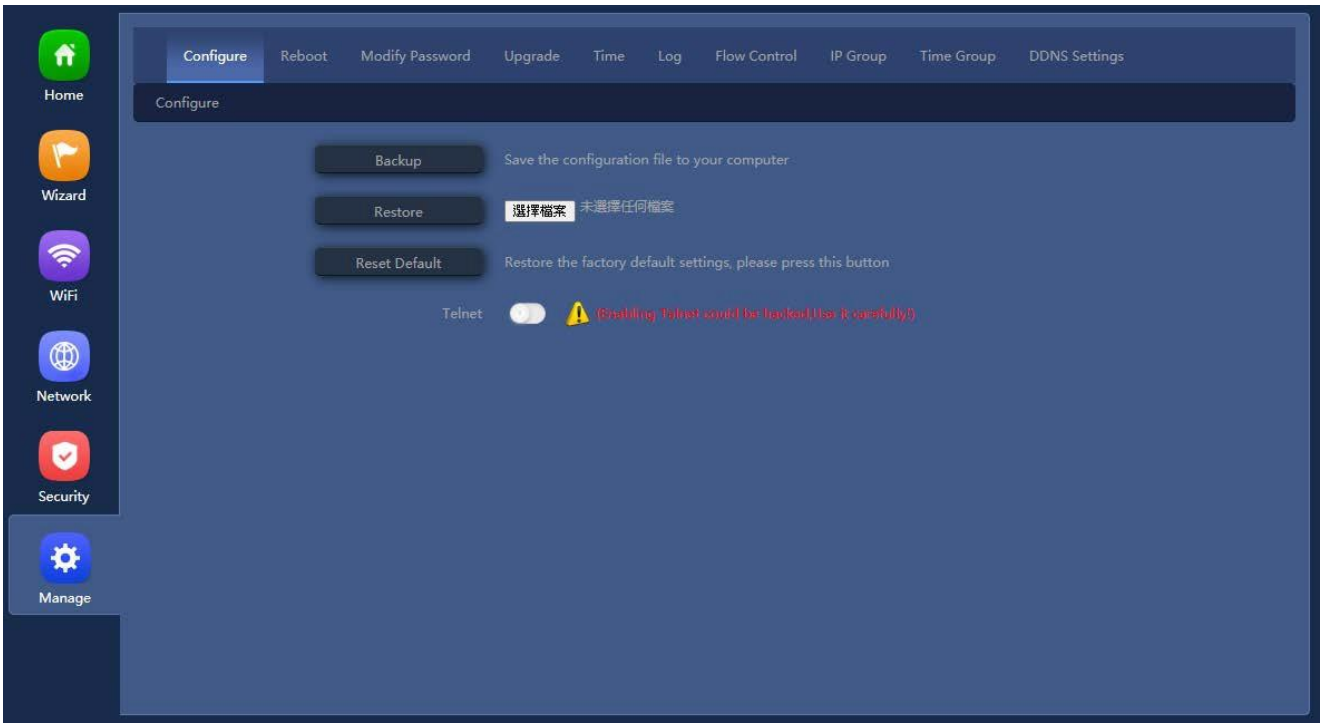


Figure 5-44 Configure

Object	Description
Backup	Press the "**Backup**" button to save the configuration file to your computer
Restore	Press the "**Restore**" button to reload the configuration file from your computer
Reset Default	Press the "**Reset Default**" button to do factory default, be careful.
Telnet	(Enabling Telnet could be hacked,Use it carefully!) Only for AirLive support team using.

5.7.2 Reboot

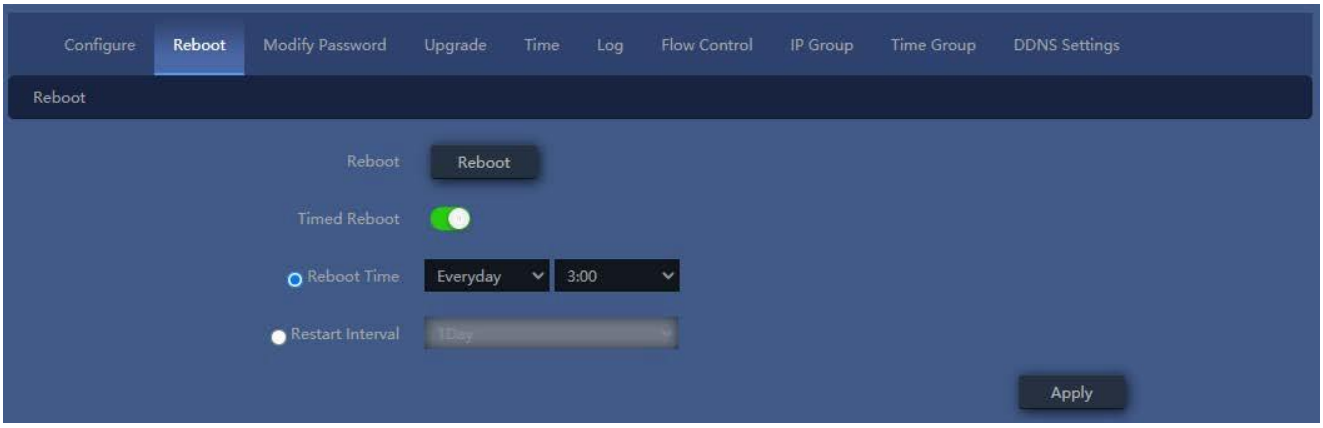


Figure 5-45 Reboot

The page includes the following fields:

Object	Description
Reboot	Press the "**Reboot**" button to restart system
Timed Reboot	Select ON (**Green**) or OFF (**Gray**) to enable or disable schedule reboot
Reboot Time	Option "**Reboot Time**" to set the date and time of the rule
Restart Interval	Option "**Restart Interval**" to select duty day of the rule

5.7.3 Modify Password

The page you can change the password.

Figure 5-46 Modify Password

5.7.4 Upgrade

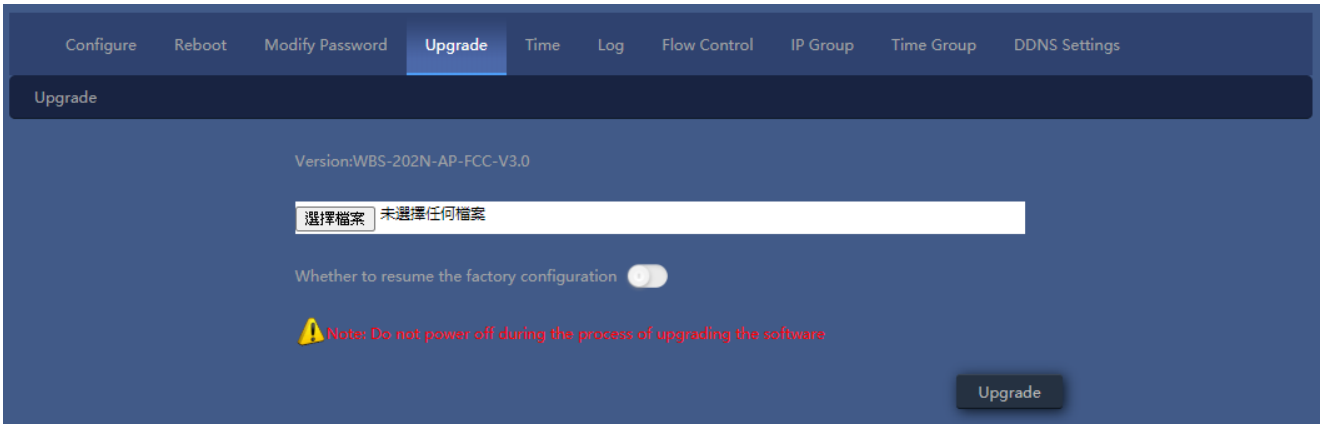


Figure 5-47 Upgrade

The page includes the following fields:

Object	Description
Select file	Press the "**Select file**" button to reload the firmware file from your computer **Be careful, choose the wrong file will crash the database**
Whether to resume the factory configuration	Select **ON (Green)** or **OFF (Gray)** to enable or disable factory default after upgrade firmware
Upgrade	Press the "**Upgrade**" button to start the process

5.7.5 Time

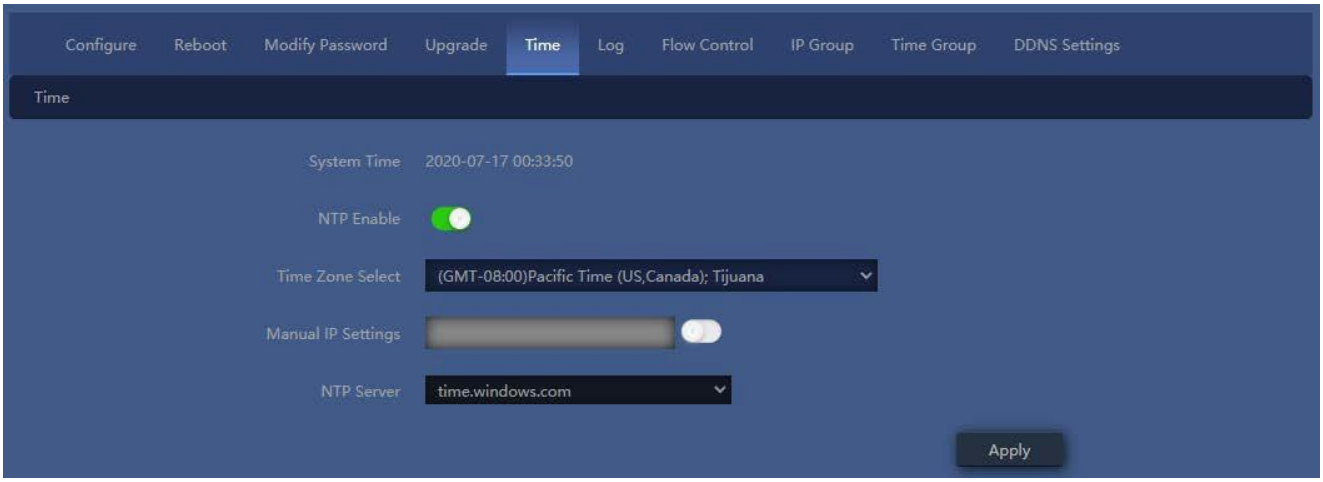


Figure 5-48 Time

The page includes the following fields:

Object	Description
System Time	Show the system time status

NTP Enable	Select **ON (Green)** or **OFF (Gray)** to enable or disable NTP
Time Zone Select	Select the time zone for GMT
Manual IP settings	Select **ON (Green)** or **OFF (Gray)** to enable or disable manual IP function
NTP Server	Select the NTP server

5.7.6 Log

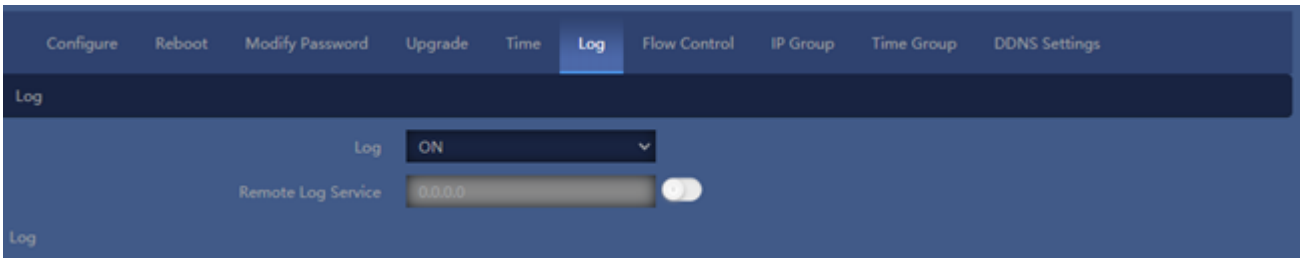


Figure 5-49 Log

The page includes the following fields:

Object	Description
Log	Select **ON (Green)** or **OFF (Gray)** to enable or disable
Remote Log Service	Select **ON (Green)** or **OFF (Gray)** to enable or disable remote log function and enter the log server IP address
Export	Press the "**Export**" button to export the log.bin file
Delete	Press the "**Delete**" button to clear the log
Refresh	Press the "**Refresh**" button to refresh the log
Apply	Press the "**Apply**" button to save the configuration

5.7.7 Flow Control

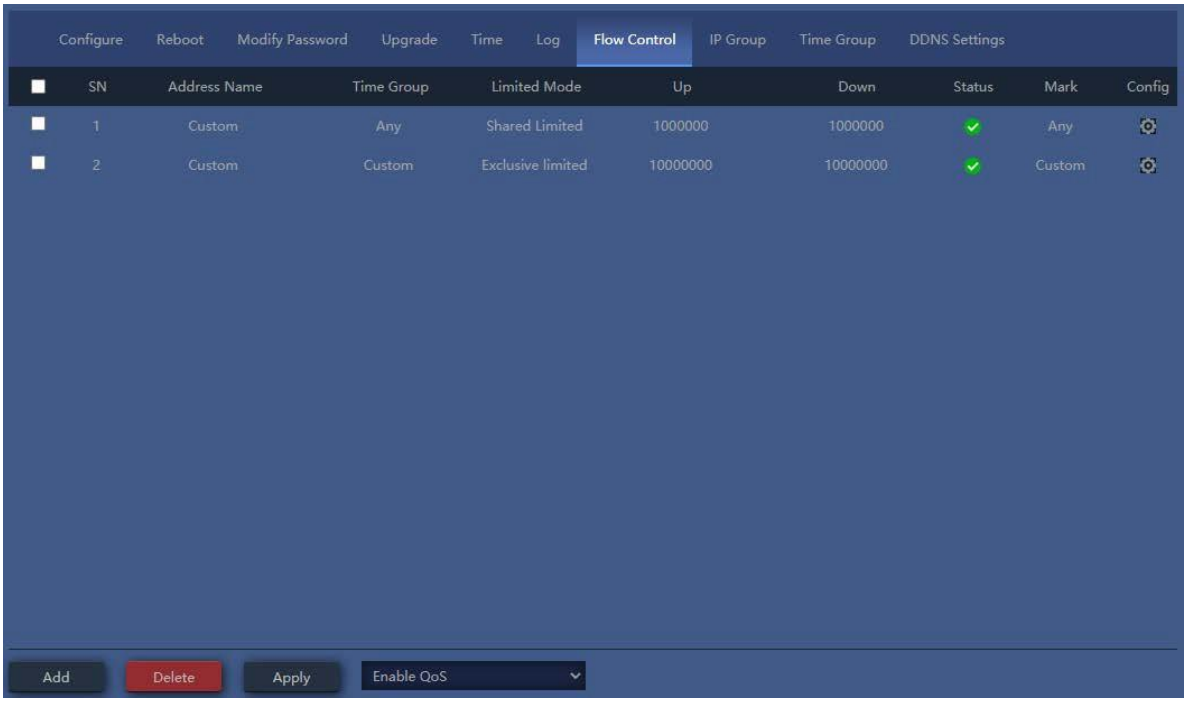


Figure 5-50 Setup Flow Control

The page includes the following fields:

Object	Description
Add	Press the "**Add**" button to add the rule in the control list
Delete	Press the "**Delete**" button to delete the rule
Apply	Press the "**Apply**" button to enable/disable the rule
Status	Select enable or disable QoS rule

Enable/disable Port Mapping function

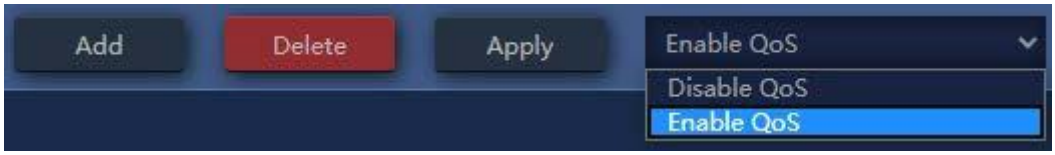


Figure 5-51 Enable or Disable QoS Rule

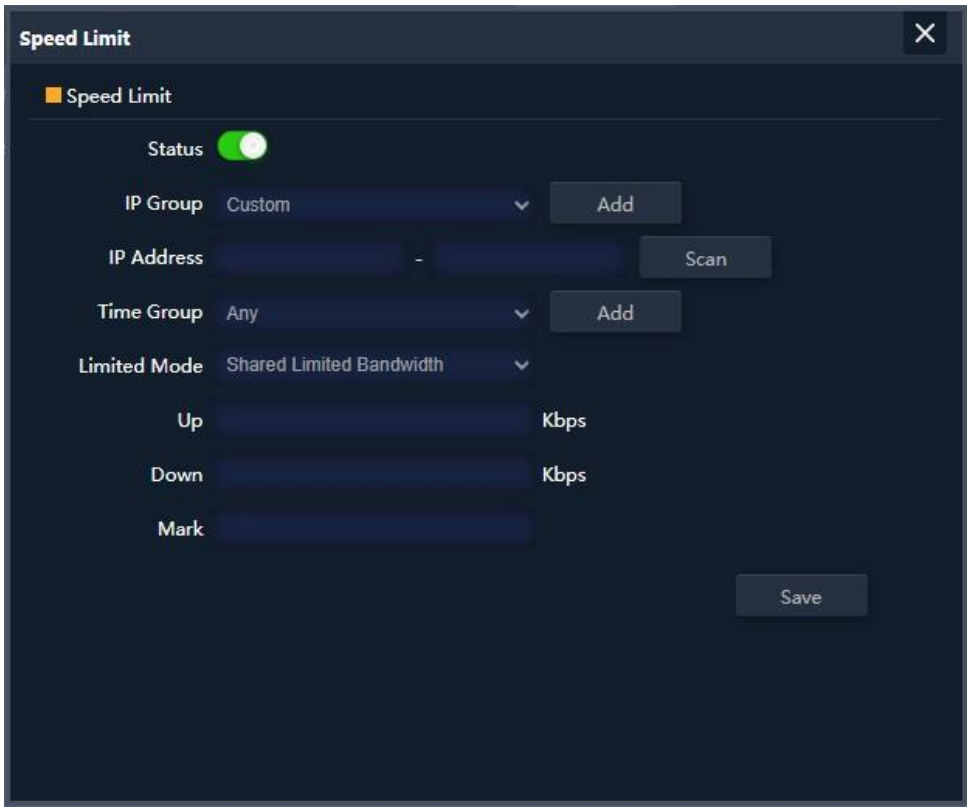


Figure 5-52 Add rule of flow control(Speed Limit)

The page includes the following fields:

Object	Description
Status	Select enable or disable flow control rule
IP Group	Select custom or Add an IP group
IP Address	Enter an IP address range or use scan to select
Time Group	Select any or custom or Add a Time group
Limited Mode	Select limited mode for shared limited bandwidth or exclusive limited bandwidth
Up	Enter the upstream limited for kbps
Down	Enter the downstream limited for kbps
Mark	Enter the mark string, or not

5.7.8 IP Group

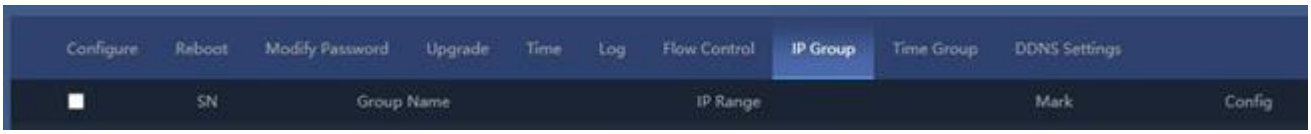


Figure 5-53 IP Group

The page includes the following fields:

Object	Description
Add	Press the "**Add**" button to add IP group in list
Delete	Press the "**Delete**" button to delete the group

Figure 5-54 Add IP Group

The page includes the following fields:

Object	Description
Group Name	Enter an IP group description
IP Address	Enter an IP address range or use scan to select
Mark	Enter the mark string, or not

5.7.9 Time Group

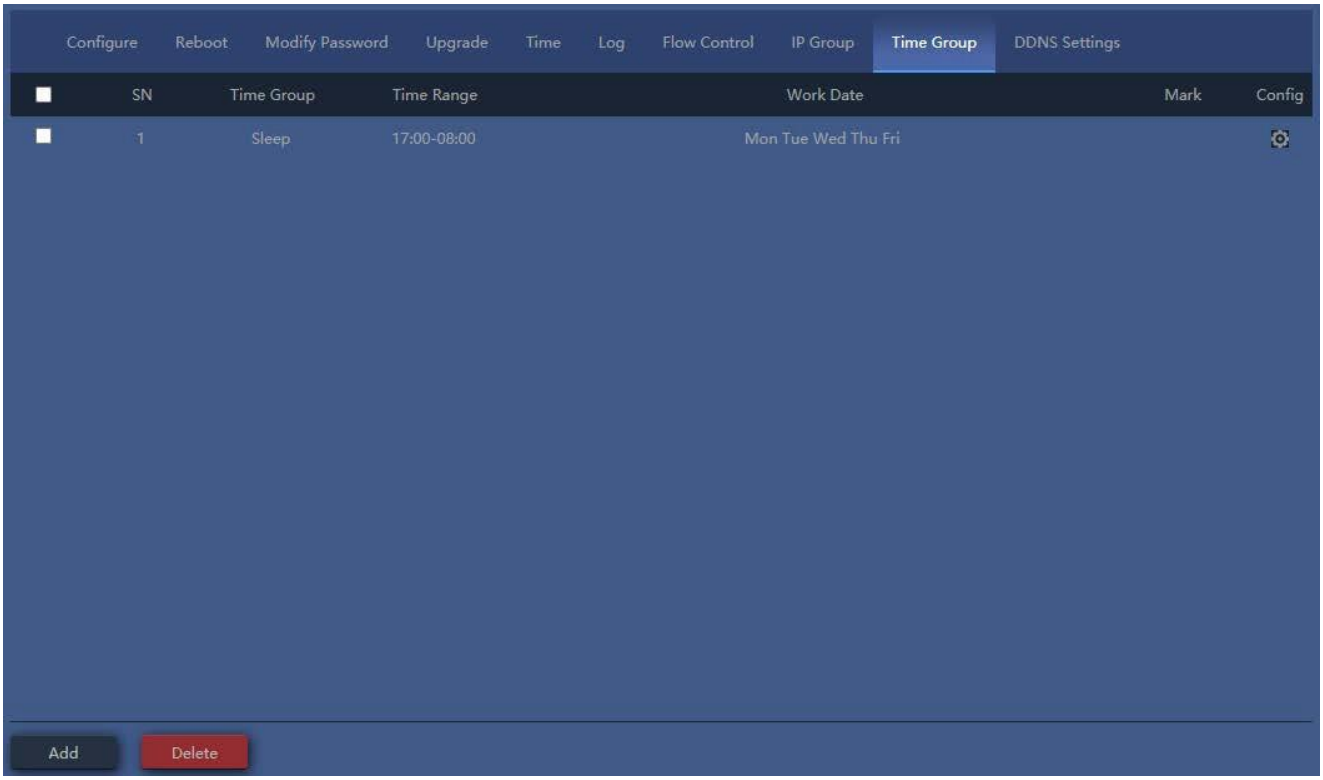


Figure 5-55 Time Group

The page includes the following fields:

Object	Description
Add	Press the "**Add**" button to add time group in list
Delete	Press the "**Delete**" button to delete the group

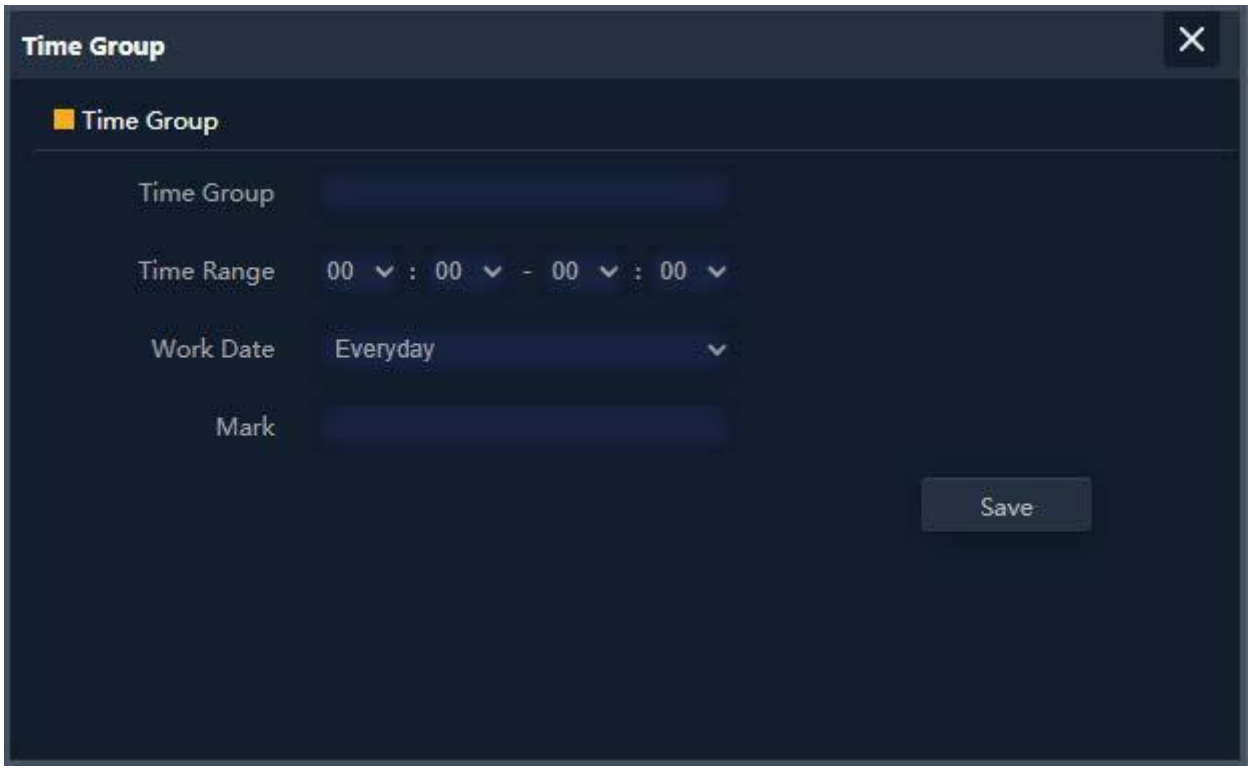


Figure 5-56 Add Time Group

The page includes the following fields:

Object	Description
Time Group	Enter a time group description
Time Range	Select start time and end time for time range
Work Date	Select workday by option table
Mark	Enter the mark string, or not

Chapter 6. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the AirMax5X II is configured to "**default**".

6.1 Windows XP (Wireless Zero Configuration)

Step 1: Right-click on the **wireless network icon** displayed in the system tray

Figure 6-1 System Tray – Wireless Network Icon

Step 2: Select [**View Available Wireless Networks**]

Step 3: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [default]

(2) Click the [**Connect**] button

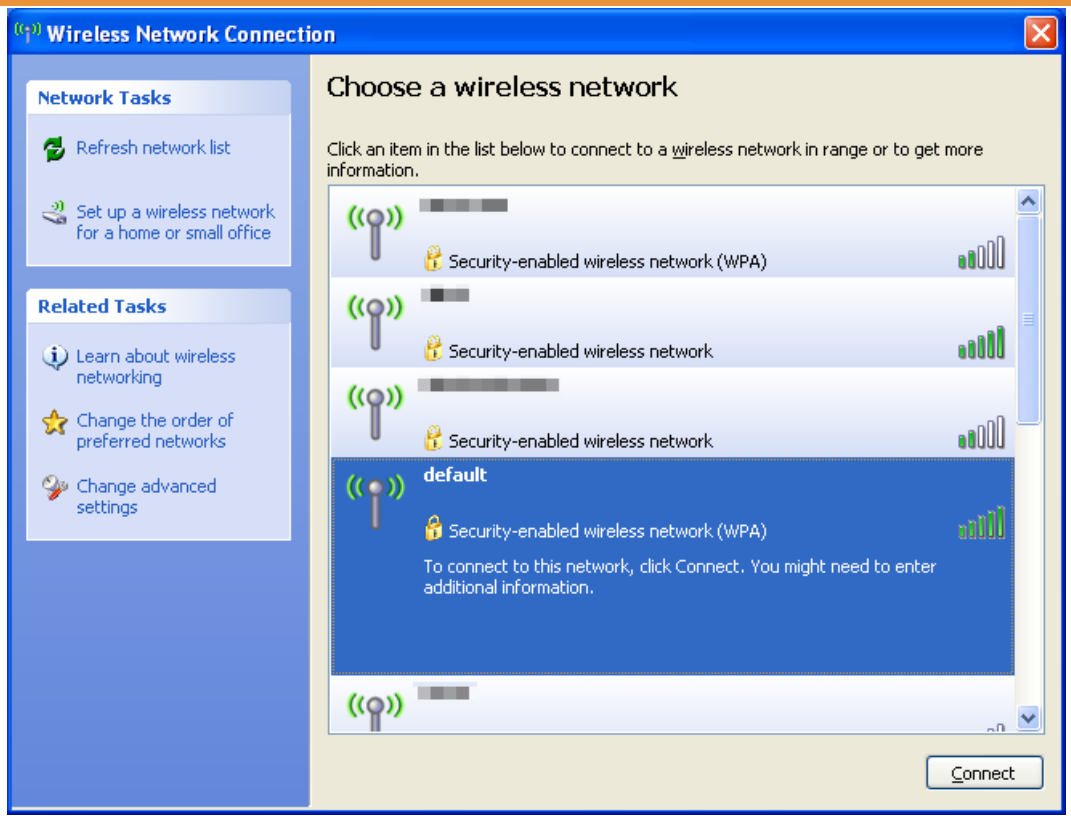


Figure 6-2 Choosing a Wireless Network

Step 4: Enter the **encryption key** of the wireless AP

(1) The Wireless Network Connection box will appear

(2) Enter the encryption key that is configured in section 5.7.2.1

(3) Click the [Connect] button

Figure 6-3 Entering the Network Key

Step 5: Check if "**Connected**" is displayed

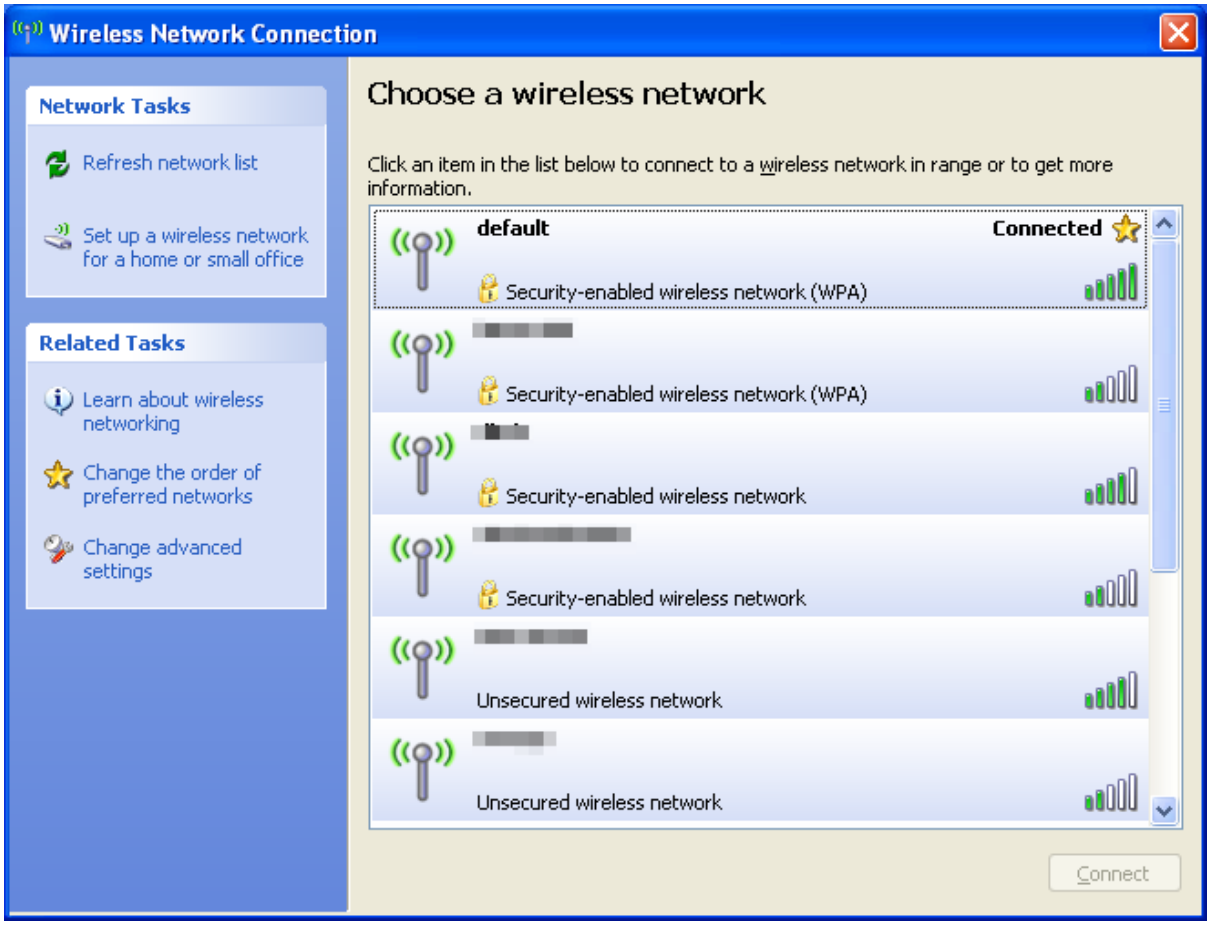


Figure 6-4 Choosing a Wireless Network -- Connected

Some laptops are equipped with a “Wireless ON/OFF” switch for the internal wireless LAN. Make sure the hardware wireless switch is switched to “ON” position.

6.2 Windows 7 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 that can be used to detect and connect to wireless network. This built-in wireless network connection tool is similar to wireless zero configuration tool in Windows XP.

Step 1: Right-click on the **network icon** displayed in the system tray

Figure 6-5 Network Icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [**default**]

(2) Click the [**Connect**] button

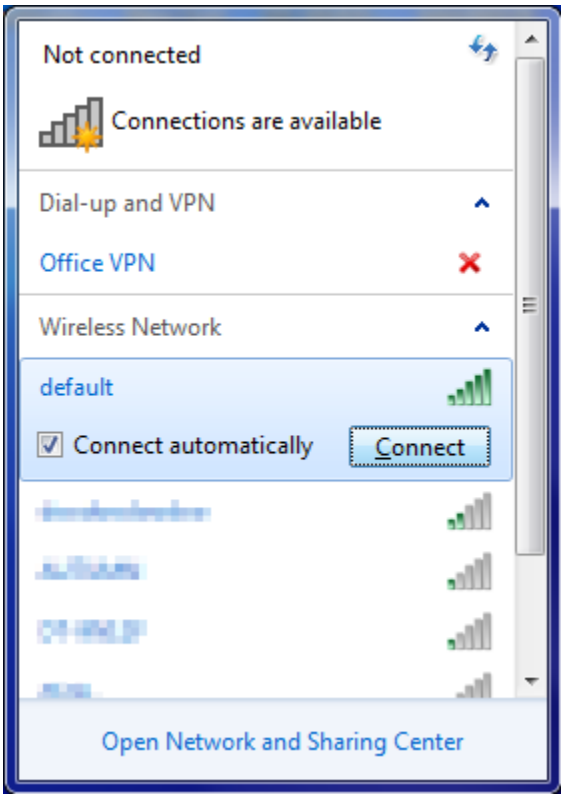


Figure 6-6 WLAN AutoConfig

Note

If you will be connecting to this Wireless AP in the future, check [**Connect automatically**].

Step 4: Enter the **encryption key** of the wireless AP

(1) The Connect to a Network box will appear

(2) Enter the encryption key that is configured

(3) Click the [OK] button

Figure 6-7 Typing the Network Key

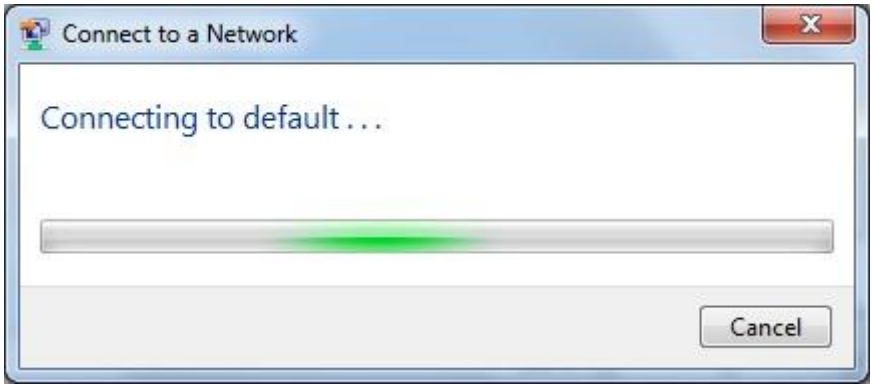


Figure 6-8 Connecting to a Network

Step 5: Check if "**Connected**" is displayed

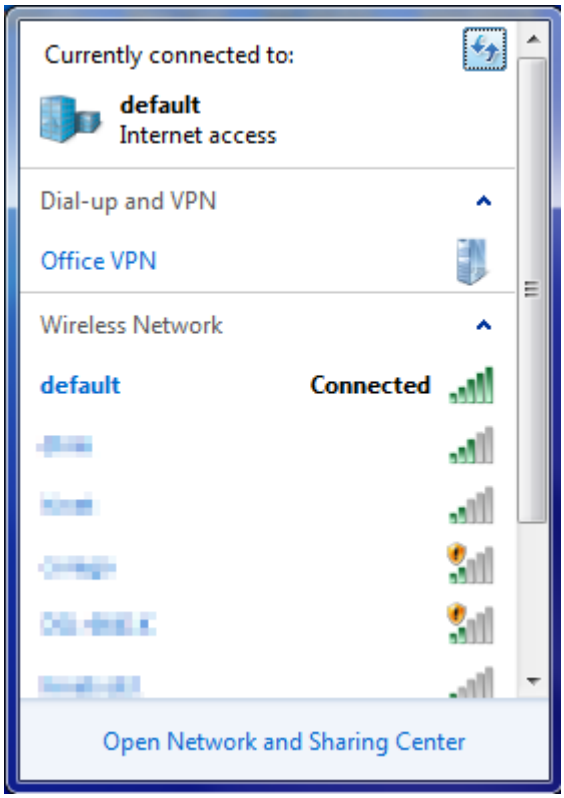


Figure 6-9 Connected to a Network

6.3 Mac OS X 10.x

In the following sections, the default SSID of the AirMax5X II is configured to "default".

Step 1: Right-click on the **network icon** displayed in the system tray

The AirPort Network Connection menu will appear

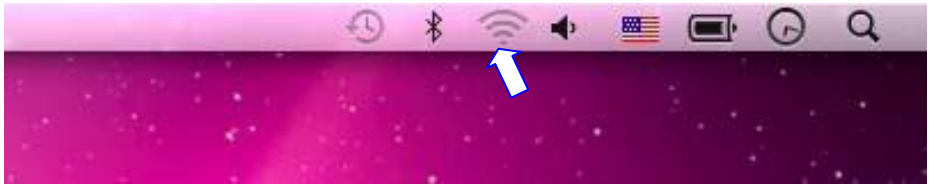


Figure 6-10 Mac OS – Network Icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select and SSID [**default**]

(2) Double-click on the selected SSID

Figure 6-11 Highlighting and Selecting the Wireless Network

Step 4: Enter the **encryption key** of the wireless AP

(1) Enter the encryption key that is configured

(2) Click the [OK] button

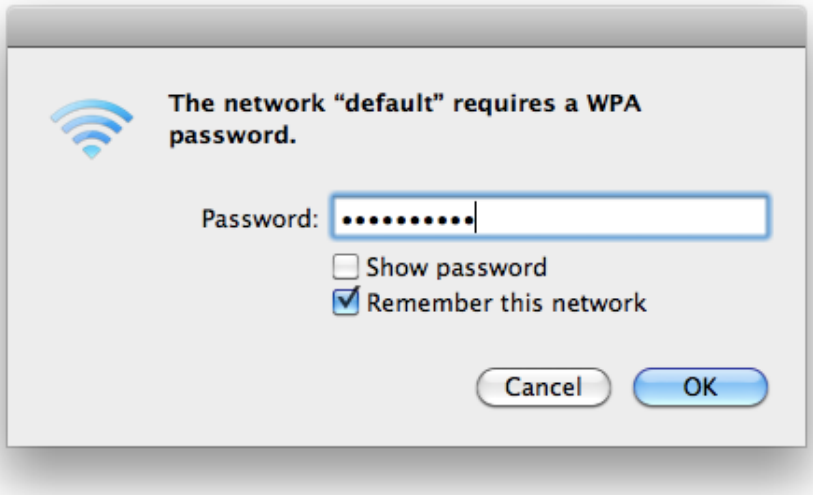


Figure 6-12 Enter the Password

Note

If you will be connecting to this Wireless AP in the future, check [**Remember this network**].

Step 5: Check if the AirPort is connected to the selected wireless network.

If "Yes", then there will be a "check" symbol in front of the SSID.

Figure 6-13 Connected to the Network

There is another way to configure the MAC OS X wireless settings:

Step 1: Click and open the [**System Preferences**] by going to **Apple** > **System Preference** or **Applications**

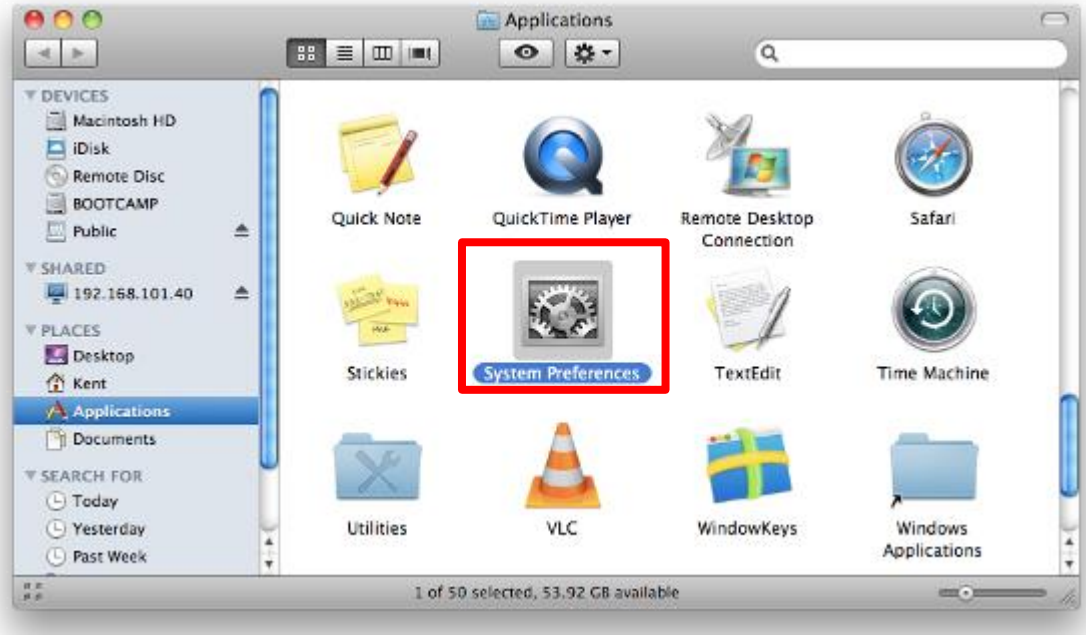


Figure 6-14 System Preferences

Step 2: Open **Network Preference** by clicking on the [**Network**] icon

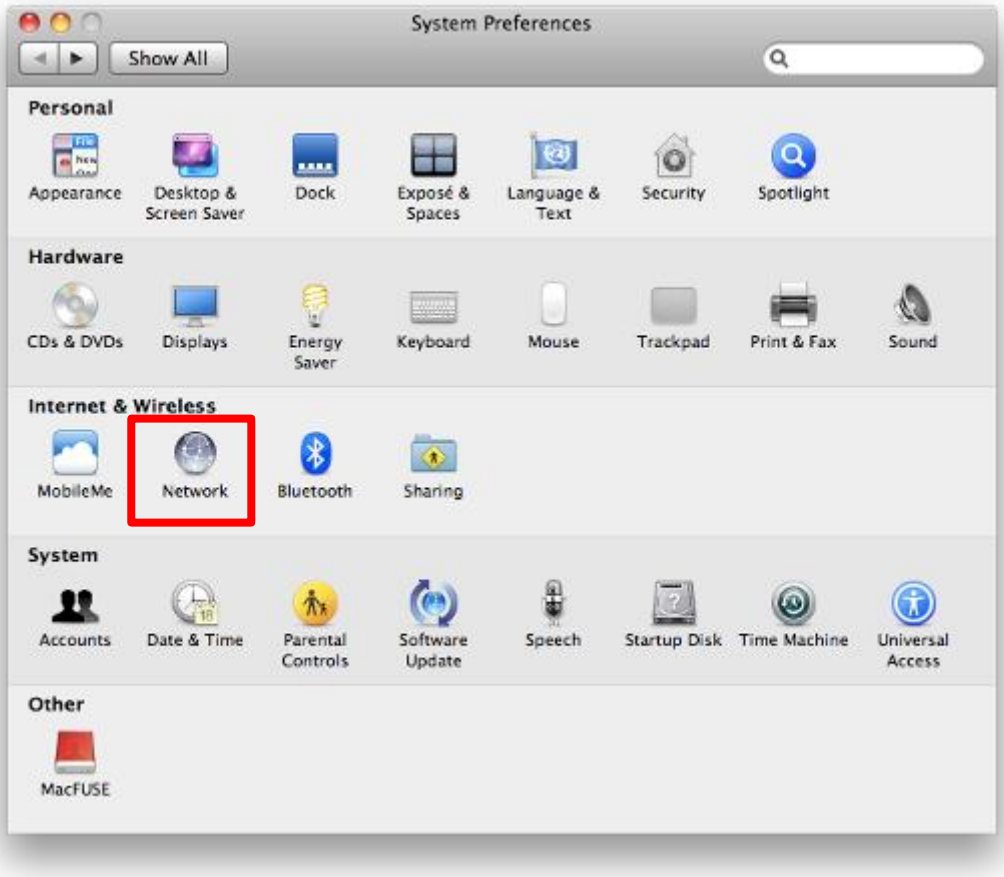


Figure 6-15 System Preferences -- Network

Step 3: Check Wi-Fi setting and select the available wireless network

(1) Choose the **AirPort** on the left-menu (make sure it is ON)

(2) Select Network Name [**default**] here

If this is the first time to connect to the Wireless AP, it should show “Not network selected”.

Figure 6-16 Selecting the Wireless Network

6.4 iPhone/iPod Touch/iPad

In the following sections, the **default SSID** of the AirMax5X II is configured to "**default**".

Step 1: Tap the [**Settings**] icon displayed in the home screen

Figure 6-17 iPhone – Settings icon

Step 2: Check Wi-Fi setting and select the available wireless network

(1) Tap [**General**] \ [**Network**]

(2) Tap [**Wi-Fi**]

If this is the first time to connect to the Wireless AP, it should show "Not Connected".

Figure 6-18 Wi-Fi Setting

Figure 6-19 Wi-Fi Setting – Not Connected

Step 3: Tap the target wireless network (SSID) in "**Choose a Network…**"

(1) Turn on Wi-Fi by tapping "**Wi-Fi**"

(2) Select SSID [**default**]

Figure 6-20 Turning on Wi-Fi

Step 4: Enter the **encryption key** of the Wireless AP

(1) The password input screen will be displayed

(2) Enter the encryption key that is configured

(3) Tap the [**Join**] button

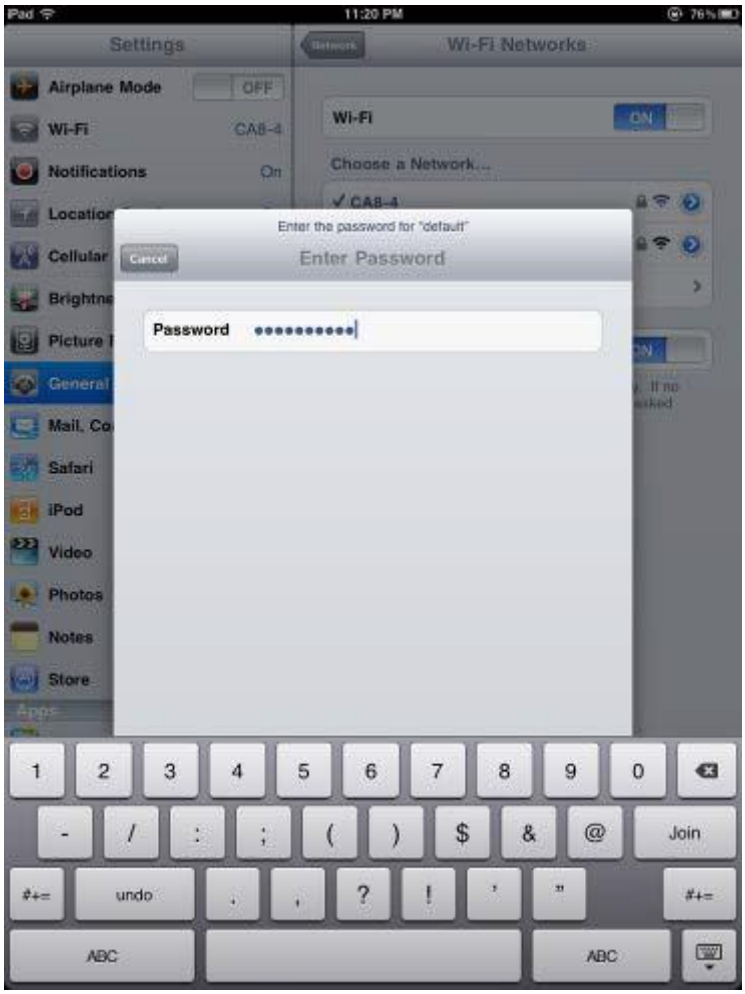


Figure 6-21 iPhone -- Entering the Password

Step 5: Check if the device is connected to the selected wireless network.

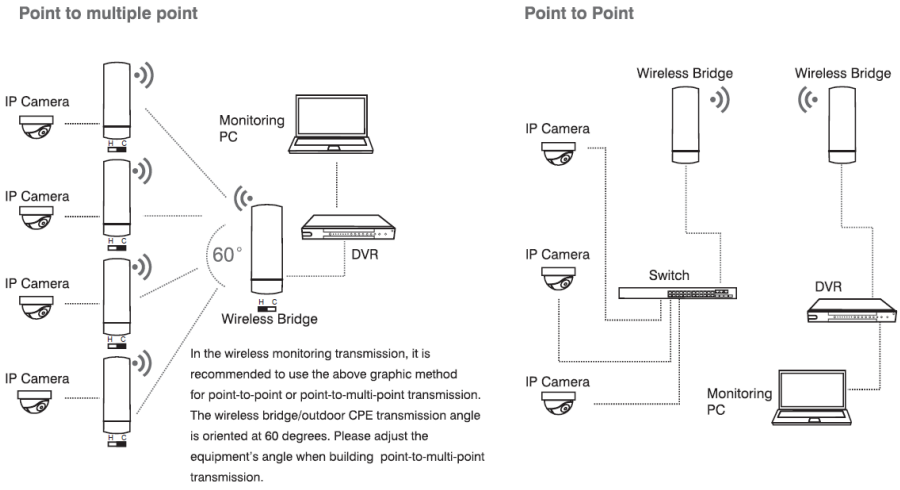
If “Yes”, then there will be a “check” symbol in front of the SSID.

Figure 6-22 iPhone -- Connected to the Network

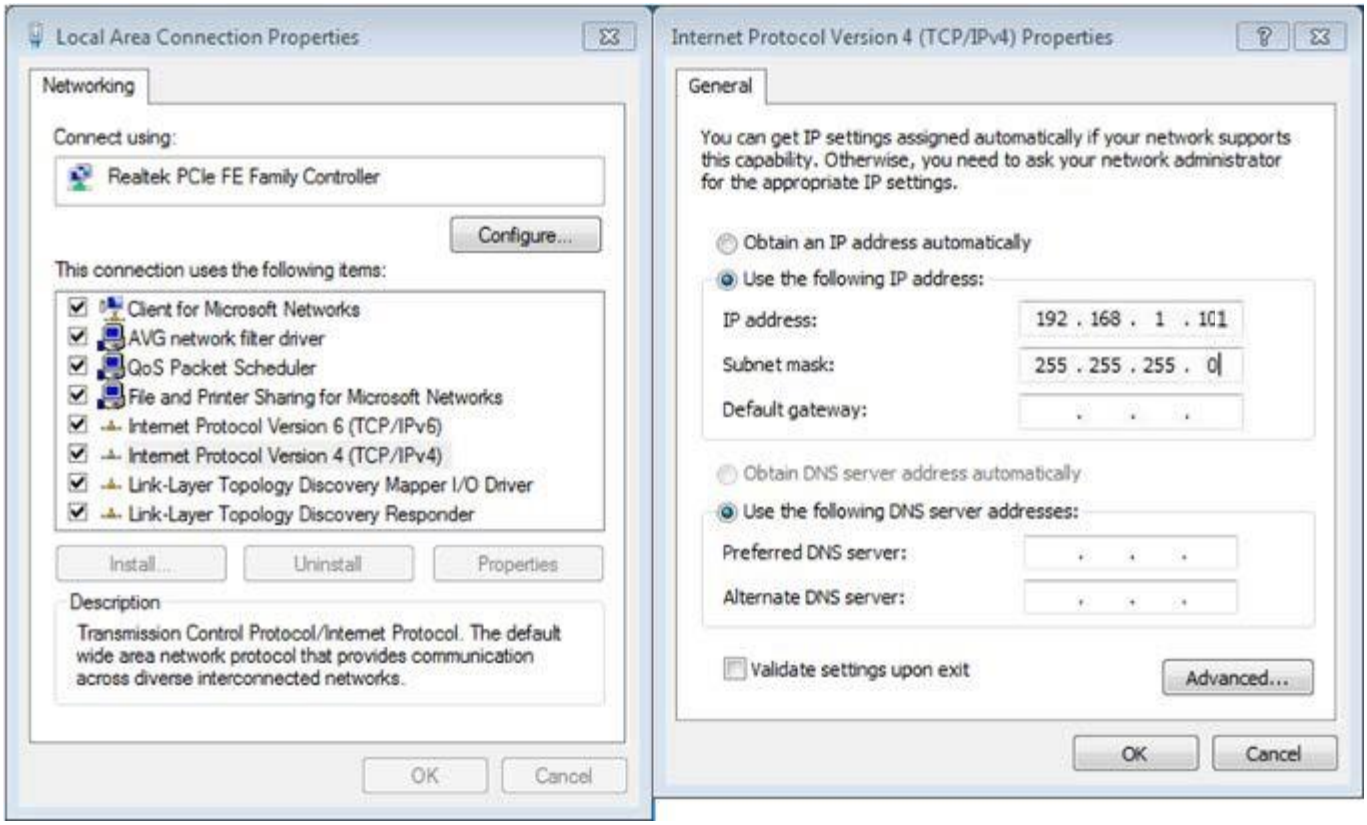
Appendix A: FAQs

Q1: How to set up the AP Client Connection

Topology:



Step1. Use static IP in the PCs that are connected with AP-1(Site-1) and AP-2(Site-2). In this case, Site-1 is "**192.168.1.101**", and Site-2 is "**192.168.1.200**".

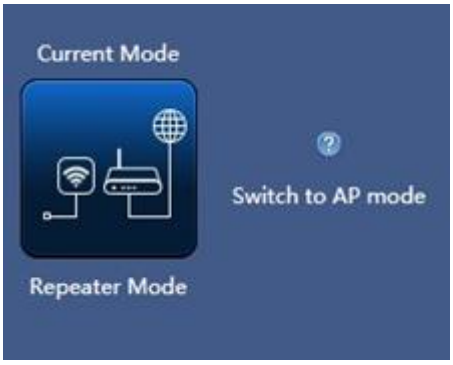


Step2. In AP-2, change the PtP switch to slave, the default IP is **192.168.1.100**.

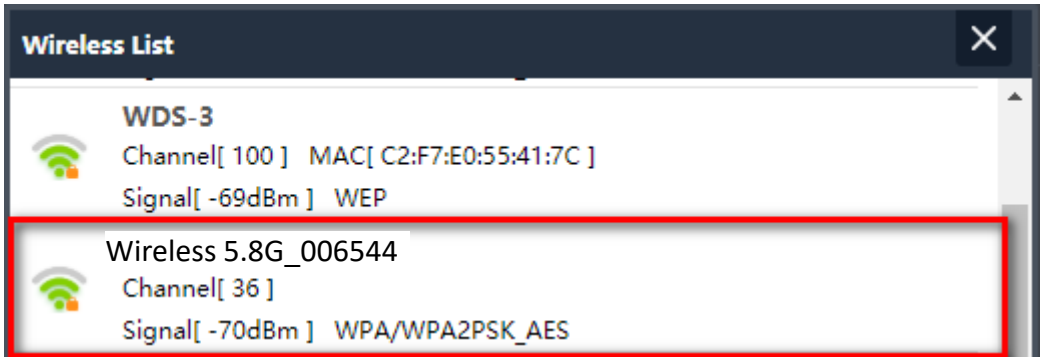
Step 3. In AP-1, go to "**Wizard**" to configure it to **AP Mode**. In AP-2, configure it to **Repeater Mode**.

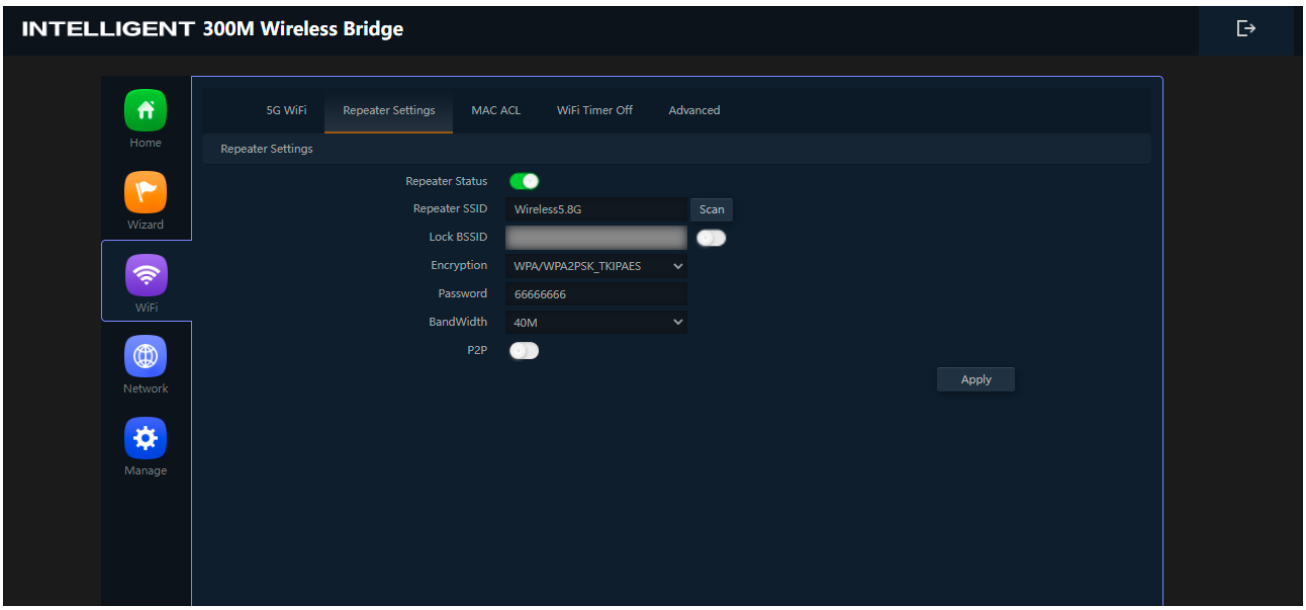
AP-1

AP-2



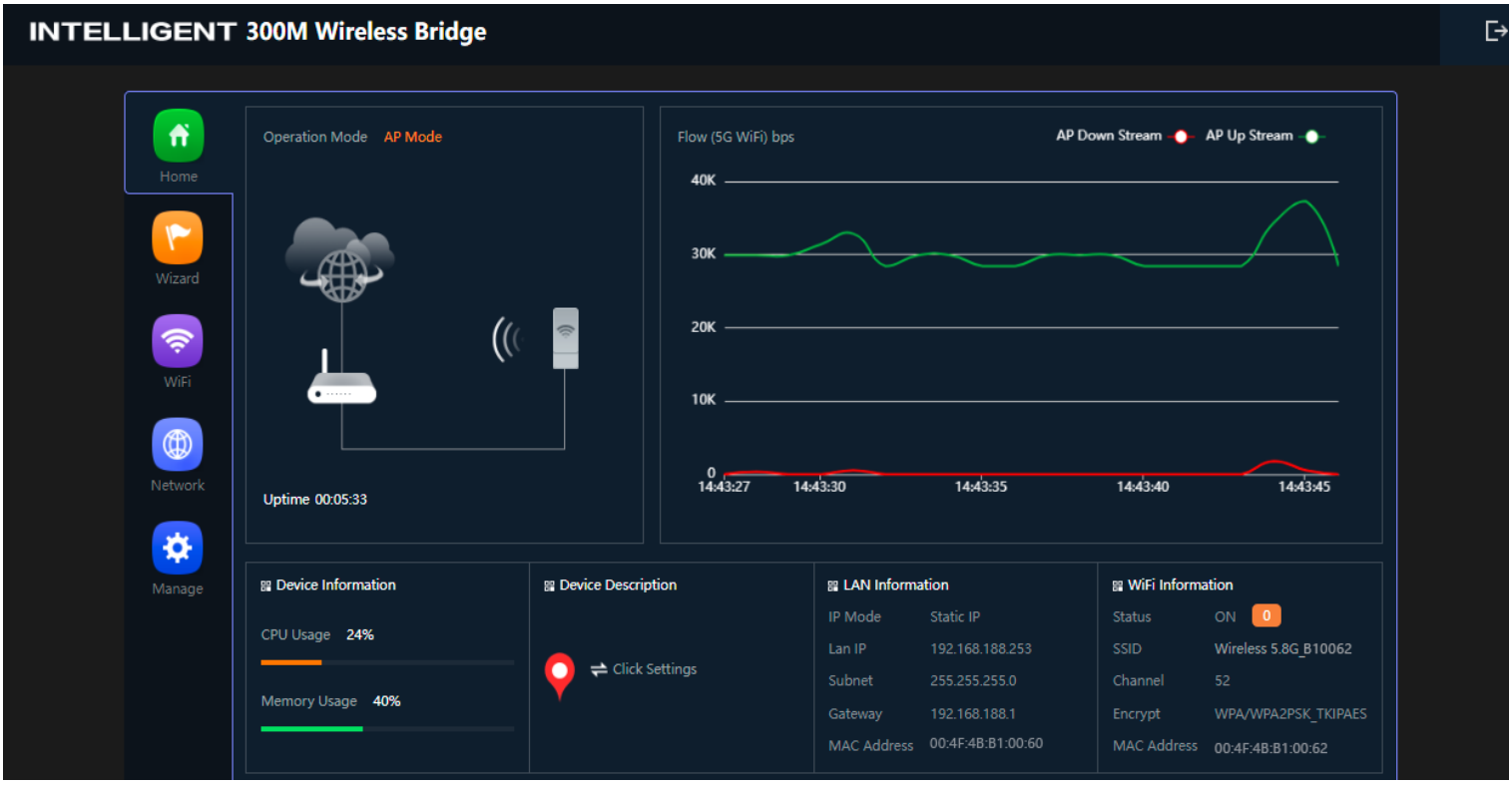
Step 4. In AP-2, press **Scan AP** to search the AP-1. You can also enter the MAC address, SSID, encryption and bandwidth if you know what they are.





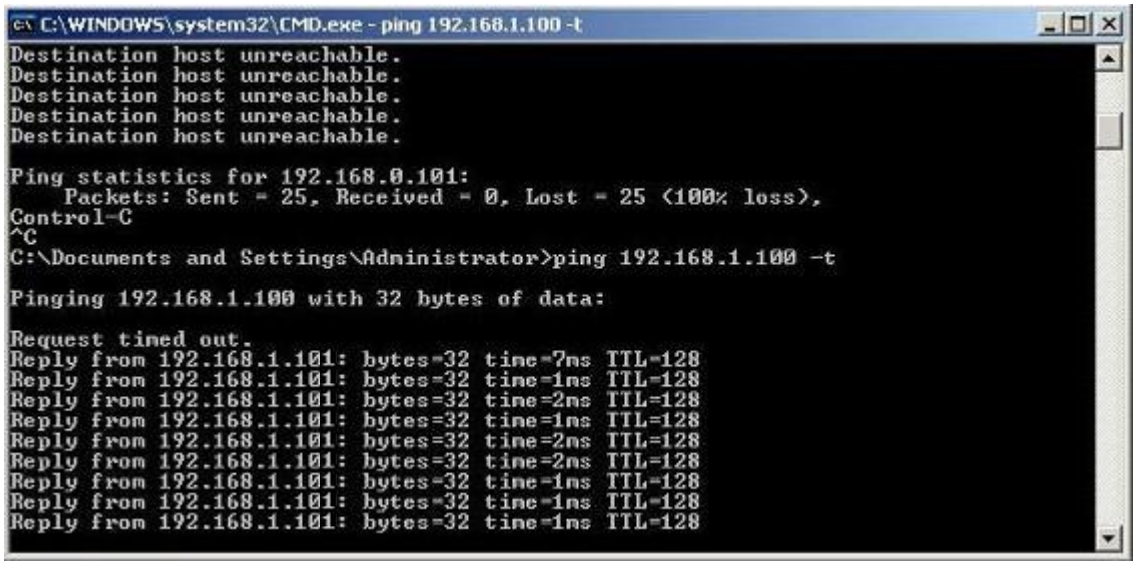
Step 5. Click "**Next**" to finish the setting. (The default Password is "**12345678**")

Step 6. Click "**Device Status**" to check connection status.

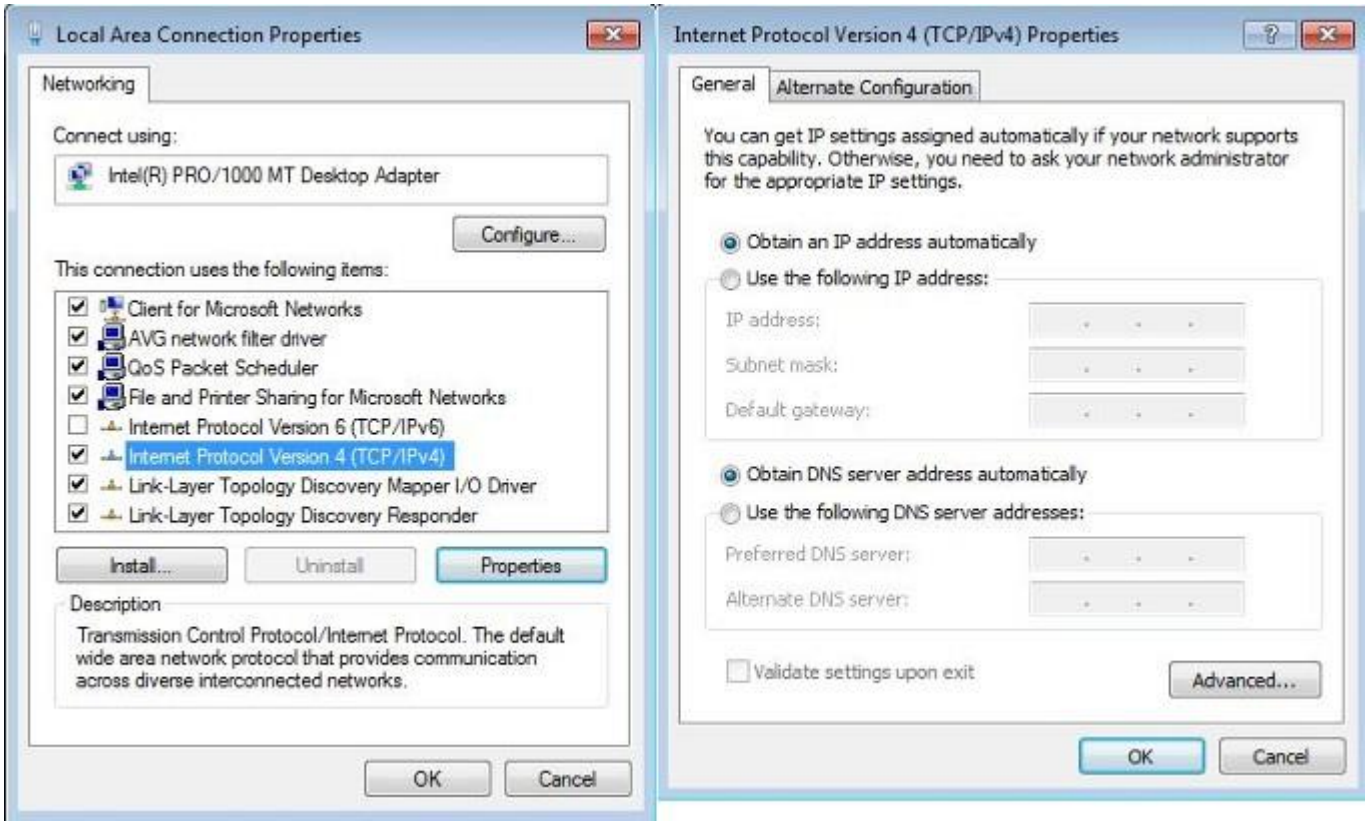


Step 7. Use command line tool to ping each other to ensure the link is successfully established.

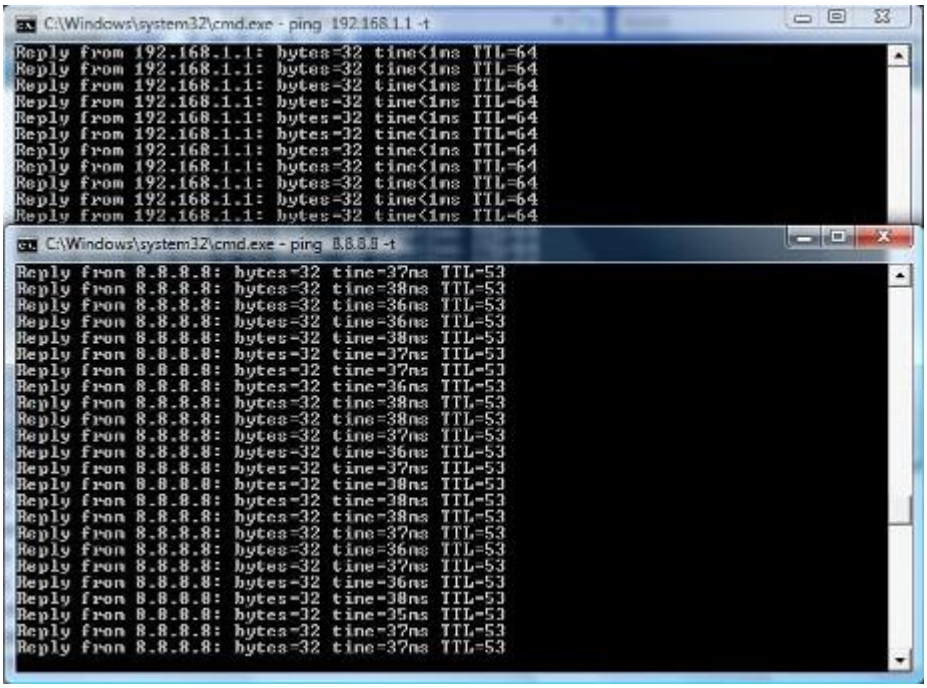
From Site-1, ping 192.168.1.200; and in Site-2, ping 192.168.1.101.



Step 8. Configure the TCP/IP settings of Site-2 to "**Obtain an IP address automatically**".



Step 9. Use command line tool to ping the DNS (e.g., Google) to ensure Site-2 can access internet through the wireless connection.



Note

The following hints should be noted:

1) The encryption method must be the same as that of both sites if configured.
2) Both sites should be Line-of-Sight.
3) For the short distance connection less than 1km, please reduce the "RF Output Power" of both sites.
4) For the long-distance connection over 1km, please adjust the "Distance" to the actual distance or double the actual distance.